FrameSaver® SLV

9126, 9126-II, and 9128-II CSU/DSU, and 9126-II Router

User's Guide

Document No. 9128-A2-GB20-80

September 2002

PARADYNE®

Copyright © 2002 Paradyne Corporation.
All rights reserved.
Printed in U.S.A.

Notice

This publication is protected by federal copyright law. No part of this publication may be copied or distributed, transmitted, transcribed, stored in a retrieval system, or translated into any human or computer language in any form or by any means, electronic, mechanical, magnetic, manual or otherwise, or disclosed to third parties without the express written permission of Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773.

Paradyne Corporation makes no representation or warranties with respect to the contents hereof and specifically disclaims any implied warranties of merchantability or fitness for a particular purpose. Further, Paradyne Corporation reserves the right to revise this publication and to make changes from time to time in the contents hereof without obligation of Paradyne Corporation to notify any person of such revision or changes.

Changes and enhancements to the product and to the information herein will be documented and issued as a new release to this manual.

Warranty, Sales, Service, and Training Information

Contact your local sales representative, service representative, or distributor directly for any help needed. For additional information concerning warranty, sales, service, repair, installation, documentation, training, distributor locations, or Paradyne worldwide office locations, use one of the following methods:

- **Internet:** Visit the Paradyne World Wide Web site at **www.paradyne.com**. (Be sure to register your warranty at **www.paradyne.com/warranty**.)
- **Telephone:** Call our automated system to receive current information by fax or to speak with a company representative.
  - Within the U.S.A., call 1-800-870-2221
  - Outside the U.S.A., call 1-727-530-2340

Document Feedback

We welcome your comments and suggestions about this document. Please mail them to Technical Publications, Paradyne Corporation, 8545 126th Ave. N., Largo, FL 33773, or send e-mail to **userdoc@paradyne.com**. Include the number and title of this document in your correspondence. Please include your name and phone number if you are willing to provide additional clarification.

Trademarks

ACCULINK, COMSPHERE, FrameSaver, Hotwire, MVL, NextEDGE, OpenLane, and Performance Wizard are registered trademarks of Paradyne Corporation. GranDSLAM, GrandVIEW, ReachDSL, and TruePut are trademarks of Paradyne Corporation. All other products and services mentioned herein are the trademarks, service marks, registered trademarks, or registered service marks of their respective owners.

Patent Notification

FrameSaver products are protected by U.S. Patents: 5,550,700 and 5,654,966. Other patents are pending.

Contents

About This Guide

1 About the FrameSaver SLV

2 User Interface and Basic Operation

3 Configuration Procedures

4 Configuration Options

5 Configuring the FrameSaver SLV Router

6 Security and Logins

7 Operation and Maintenance

8 Troubleshooting

9 Setting Up OpenLane for FrameSaver Devices and Activating SLM Features

10 Setting Up NetScout Manager Plus for FrameSaver Devices

11 Setting Up Network Health for FrameSaver Devices

A Menu Hierarchy

B SNMP MIBs and Traps, and RMON Alarm Defaults

C Router CLI Commands, Codes, and Designations

D Router Command Line Summaries and Shortcuts

E Connectors, Cables, and Pin Assignments

F Technical Specifications

G Equipment List

Index

About This Guide

Purpose and Intended Audience

This document contains information needed to properly set up, configure, and verify operation of the FrameSaver SLV (Service Level Verifier) 9126, 9126-II, and 9128-II CSU/DSU, and 9126-II Router running firmware release 2.0.3 or above. It is intended for system designers, engineers, administrators, and operators.

You must be familiar with the functional operation of digital data communications equipment and frame relay networks.

Document Organization

Section	**Description**
Chapter 1, *About the FrameSaver SLV*	Identifies how the FrameSaver SLV 9126, 9126-II, and 9128-II CSU/DSU, and 9126-II Router, fit into Paradyne's Service Level Management (SLM) solution, and describes their features.
Chapter 2, *User Interface and Basic Operation*	Shows how to navigate the menu-driven user interface.
Chapter 3, *Configuration Procedures*	Shows how to access and save configuration options.
Chapter 4, *Configuration Options*	Provides configuration information for the FrameSaver SLV 9126, 9126-II, and 9128-II CSU/DSU, and 9126-II Router.
Chapter 5, *Configuring the FrameSaver SLV Router*	Describes the router's interfaces and features, and shows typical setups and configurations.
Chapter 6, *Security and Logins*	Provides procedures for controlling access to the FrameSaver SLV and setting up logins.
Chapter 7, *Operation and Maintenance*	Provides procedures to display unit identification information and perform file transfers, as well as how to display and interpret status and statistical information.
Chapter 8, *Troubleshooting*	Provides device problem resolution, alarm, and other information, as well as troubleshooting and test procedures.

Section	Description
Chapter 9, *Setting Up OpenLane for FrameSaver Devices and Activating SLM Features*	Identifies where installation and setup information is located and how FrameSaver units are supported.
Chapter 10, *Setting Up NetScout Manager Plus for FrameSaver Devices*	Describes setup of the NetScout Manager Plus application so it supports FrameSaver units, and so you can change alarm and history file defaults.
Chapter 11, *Setting Up Network Health for FrameSaver Devices*	Describes setup of Concord's Network Health application so reports can be created for FrameSaver units, and identifies those reports that apply to FrameSaver units.
Appendix A, *Menu Hierarchy*	Contains a graphical representation of how the user interface screens are organized.
Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*	Identifies the MIBs supported and how they can be downloaded, describes the unit's compliance with SNMP format standards and with its special operational trap features, and describes the RMON-specific user history groups, and alarm and event defaults.
Appendix C, *Router CLI Commands, Codes, and Designations*	Describes the configuration options available for the router, and the minimum access level for each command.
Appendix D, *Router Command Line Summaries and Shortcuts*	Provides a summary of router CLI commands, showing syntax and defaults.
Appendix E, *Connectors, Cables, and Pin Assignments*	Shows the rear panel, tells what cables are needed, and provides pin assignments for interfaces and cables.
Appendix F, *Technical Specifications*	Technical Specifications.
Appendix G, *Equipment List*	Equipment List.
Index	Lists key terms, acronyms, concepts, and sections.

A master glossary of terms and acronyms used in Paradyne documents is available on the World Wide Web at **www.paradyne.com**. Select *Library* → *Technical Manuals* → *Technical Glossary*.

Product-Related Documents

Document Number	Document Title
Paradyne FrameSaver Documentation:	
9000-A2-GN19	*FrameSaver SLV ISDN Installation Instructions*
9000-A2-GN1D	*9000 Series Access Carrier Installation Instructions*
9126-A2-GL10	*FrameSaver SLV 9126 and 9126-II Quick Reference*
9126-A2-GL12	*FrameSaver SLV 9126-II Router Quick Reference*
9126-A2-GN10	*FrameSaver SLV 9126 1-Slot Unit Installation Instructions*
9126-A2-GN11	*FrameSaver SLV 9126-II 1-Slot Unit Installation Instructions*
9126-A2-GN12	*FrameSaver SLV 9126-II Router Installation Instructions*
9128-A2-GL10	*FrameSaver SLV 9128/9128-II Quick Reference*
9128-A2-GN10	*FrameSaver SLV 9128 1-Slot Housing-to-9000 Series Access Carrier Upgrade Instructions*
9128-A2-GN11	*FrameSaver SLV 9128/9128-II Network Access Module (NAM) Installation Instructions*
9128-A2-GN12	*FrameSaver SLV 9128/9128-II 1-Slot Unit Installation Instructions*
Paradyne OpenLane NMS Documentation:	
7800-A2-GB30	*OpenLane SLM Reports Reference Guide*
7800-A2-GB32	*OpenLane SLM Administrator's Guide*
NetScout Documentation:	
2930-170	*NetScout Probe User Guide*
2930-610	*NetScout Manager/Plus User Guide*
2930-620	*NetScout Manager/Plus & NetScout Server Administrator Guide*
2930-788	*NetScout Manager Plus Set Up & Installation Guide*
Concord Communications Documentation:	
09-10010-005	*Network Health User Guide*
09-10020-005	*Network Health Installation Guide*
09-10050-002	*Network Health – Traffic Accountant Reports Guide*
09-10070-001	*Network Health Reports Guide*

Complete Paradyne documentation for this product is available at **www.paradyne.com**. Select *Library* → *Technical Manuals.*

To order a paper copy of this manual:

- Within the U.S.A., call 1-800-PARADYNE (1-800-727-2396)
- Outside the U.S.A., call 1-727-530-8623

Conventions Used

Convention Used	**When Used**
Italic	To indicate variable information (for example, DLCI *nnnn*, where *nnnn* denotes a 4-digit number).
Menu sequence:	To provide an abbreviated method for indicating the selections to be made from a menu or selections from within a menu before performing a procedural step. For example, *Main Menu → Status → System and Test Status* indicates that you should select Status from the Main Menu, then select System and Test Status.
(Path:)	To provide a check point that coincides with the menu path shown at the top of the screen. Always shown within parentheses so you can verify that you are referencing the correct table (e.g., Path: main/config/alarm).
Brackets [ ]	To indicate multiple selection choices when more than one selection is available (e.g., *Performance Statistics→ Status→ [Network/Port-1]*).
Text highlighted in blue	To indicate a hyperlink to additional information when viewing this manual online. Click on the highlighted text.

About the FrameSaver SLV

1

This chapter includes the following:

System Overview

Our system solution consists of:

- FrameSaver® SLV (Service Level Verifier) units
- OpenLane® SLM (Service Level Management) system
- NetScout Manager Plus application
- Standalone NetScout Probes, if needed

This solution provides increased manageability, monitoring, and diagnostics so customers can identify problems more efficiently, troubleshoot those problems faster, and maximize their network to control costs. It is also compatible with Concord Communication’s Network Health software.

The FrameSaver SLV 9126-II Router and 9126, 9126-II, and 9128-II CSU/DSUs operate with other FrameSaver devices, and when teamed with internationally based FrameSaver devices in multinational applications, provide a complete global frame relay management solution.

CSU/DSU-Specific Features

The following features only apply to the FrameSaver SLV 9126, 9126-II, and 9128-II CSU/DSUs:

- **Two Interfaces.** Provides two interfaces for traffic:
  - Synchronous DTE port for user data
  - Ethernet Interface for management data
- **Upstream Pipelining.** Provides pipelining capability into the Wide Area Network (WAN) for reduced latency, where groups of bytes are transmitted as soon as they are received, rather than waiting for the entire frame to be collected before sending.
- **LMI Protocol Support.** Automatically detects and initializes the Local Management Interface (LMI) protocol type on the user data port.

Router-Specific Features

The following features only apply to the FrameSaver SLV 9126-II router:

- **Device Migration.** The FrameSaver SLV 9126-II Router can be converted to a FrameSaver SLV 9126-II CSU/DSU with a firmware download.
- **In-Band Router Management.** Permits the router to be managed via customer data PVCs and EDLCIs by assigning an IP address for router management that is different from the IP address generally used for the network interface.
- **Inverse ARP for User Data.** Provides Inverse ARP (Address Resolution Protocol) support for user data, as well as management data. The router responds to Inverse ARP requests, and can acquire the IP address of a FrameSaver device at the far end of a customer PVC. ARP information is retained for both customer data and management data.

- **CLI Access and Configuration.** Provides a router Command Line Interface (CLI), along with the menu-driven user interface, for configuring and managing the router. It is accessed from the Main Menu via a direct COM port connection or Telnet.

  The following features are configurable using the CLI:

  — NAT (Network Address Translation) support provides the means to bind IP addresses in a private network to addresses in a public, or global, network for transparent routing between the two domains on all PVCs. Up to 30 NAT pools are supported.

  — Routing table configuration permits configuration of static routes. Up to 32 entries can be made.

  — IP forwarding to forward multicast IP packets and customer datagrams.

  — Filtering on the Ethernet and frame relay interfaces, configurable from the CLI access list, allows the router to filter MAC frames and prevent unwanted inbound connections. Two filter access lists are supported per interface, one for the transmit and one for the receive direction.

  The following protocol is supported:

  — DHCP (Dynamic Host Configuration Protocol) support for dynamic allocation of IP addresses and automatic cleanup when a subinterface is deleted, as well as allowing multiple IP address ranges for DHCP deny capability. The DHCP server and relay cannot be enabled at the same time. Up to 253 DHCP clients can be supported. One DHCP pool of addresses, and one IP address range per pool is supported.

FrameSaver Diagnostic and SLM Feature Sets

Depending upon the model ordered, the FrameSaver unit has the basic FrameSaver frame relay and diagnostic capability, or it is enhanced with additional SLM (Service Level Management) reporting capability. These are referred to as feature sets, which provide different levels of intelligence for monitoring, managing, and reporting performance of the unit.

The two feature sets include:

- **Basic Diagnostic Feature Set.** Models with this feature set provide basic FrameSaver capabilities, which include:

  — Leased Line mode for standard DSU installation and operation

  — Device health and status

  — Layer 1 (Physical) and Layer 2 (Frame Relay) performance statistics

  — Basic physical testing and non-disruptive PVC diagnostics

  — A troubleshooting DLCI (Data Link Connection Identifier) for service provider use and remote management

  — Limited RMON (Remote Monitoring) functionality

  — Multiplexed management PVCs

  See *FrameSaver Diagnostic Feature Set* on page 1-5 for other features and additional information.

- **Advanced SLM Feature Set.** Models with this feature set provide all the basic diagnostic capability, plus advanced Service Level Management features. When additional SLV data is collected and the unit is accessed from an OpenLane SLM system, Web access to the following information is available:

  — TruePut™ Technology using Frame and Data Delivery Ratios (FDR and DDR)

  — Web browser access to all diagnostic and reporting functions

  — Historical SLA (Service Level Agreement) verification and trend reports

  — Real-time RMON (remote monitoring) alarms and configurable alarm thresholds

  — Real-time and historical network performance graphs

  — Multiplexed customer PVCs

  See *FrameSaver SLM Feature Set* on page 1-10 for more information about the additional SLM capability.

If the unit does not have the SLM feature set, full SLM capability can be activated at any time by ordering a Feature Activation Certificate. The OpenLane SLM system Release 5.3 or above is required to schedule activation of advanced SLM features in units, and to manage activations.

To obtain a Feature Activation Certificate, provide the model to be upgraded, your OpenLane system license key number, and the number of FrameSaver units to be upgraded to SLM capability. You can order the certificate for a single unit or for many units. Your Feature Activation Certificate will include an Activation Certificate Number, the Feature Group Number for the additional SLM features, your OpenLane license key number, and the number of device activations ordered.

When the Feature Activation Certificate arrives, add the Activation Certificate Number to your OpenLane SLM application's database. Activations can occur at any time, for as many units as desired, until no activations remain for the certificate. When ready to activate units, simply select the units to be activated and schedule the activations. The activations occur when scheduled, and OpenLane updates the certificate information. The OpenLane system also provides a Certificate Summary Report to assist you in the management of the certificate.

FrameSaver Diagnostic Feature Set

A FrameSaver SLV unit with the basic diagnostic feature set provides the following:

- **Easy Installation.** Provides a straightforward installation menu that requires minimal configuration to get the unit up and running quickly, and to set up remote configuration and management via Telnet access from the NOC (Network Operations Center).

- **Frame Relay Aware Management.** Supports diagnostic and network management features over the frame relay network. The unit's frame relay capability also supports:

  - Inband management channels over the frame relay network using dedicated PVCs.

  - Unique nondisruptive diagnostics.

  - CIR monitoring on a PVC basis.

  - Multiple PVCs on an interface.

  - Multiplexing management PVCs with user data PVCs.

  - Multiplexing multiple PVCs going to the same location onto a single network PVC.

- **Router Independence.** Unique diagnostics, performance monitoring, PVC-based in-band network management, and SNMP connectivity is not dependent upon external routers, cables, or LAN adapters.

- **Inverse ARP and Standard RIP Support.** Provides Inverse ARP (Address Resolution Protocol) support so the frame relay router at one end of a management PVC can acquire the IP address of a FrameSaver unit at the other end of the PVC. Standard RIP (Routing Information Protocol) allows the router to automatically learn the routes to all FrameSaver units connected to that FrameSaver unit.

- **Security.** Provides multiple levels of security to prevent unauthorized access to the unit.

- **Auto-Configuration**. Provides the following automatic configuration features:
  - — Time Slot Discovery – For automatic configuration of all network DS0 assignments.
  - — Frame Relay Discovery – For automatic discovery of network DLCIs and configuration of a user data port DLCI, the PVC connection, and a management PVC, which is multiplexed with user data DLCIs.
  - — LMI Protocol Discovery – For automatic configuration of the protocol being used by the network.
  - — DLCI Deletion – For automatic removal of configuration of unused DLCIs from the unit's configuration and statistical databases.
  - — CIR Determination – For automatic recalculation of the committed rate measurement interval (Tc) and excess burst size (Be) when a DLCI's CIR changes.
  - — Excess burst size (Be) and committed burst size (Bc) are recalculated when Committed Burst Size Bc (Bits) is set to CIR. The committed rate measurement interval (Tc) is recalculated when Committed Burst Size Bc (Bits) is set to Other.

- **Maximum Number of PVCs and Management PVCs Supported.**

Feature	FrameSaver SLV 9126-II Router	FrameSaver SLV 9126 CSU/DSU	FrameSaver SLV 9126-II CSU/DSU	FrameSaver SLV 9128-II CSU/DSU
Through Connections (PVCs)	8	16	64	120
Dedicated Management PVCs	2	2	2	2

- **Multiplexed Management PVCs.** Provides a method of multiplexing management data with customer data transparently over a single PVC (Permanent Virtual Circuit) when FrameSaver devices are at each end of the circuit. This feature also makes it possible to run nondisruptive PVC tests.

- **Extensive Testing Capability.** Provides a variety of tests to identify and diagnose device and network problems, including nondisruptive PVC loopbacks and end-to-end connectivity. Tests can be commanded from the unit's menu-driven user interface or the OpenLane system.

  These tests include V.54 or FT1-ANSI data channel loopback support so the frame relay network service provider can perform a physical loopback from its own switch without having to contact the local service provider for loopback activation.

- **LMI Packet Capture.** Provides a way of uploading data that has been captured in a trace file so the data can be uploaded and transferred to a Network Associates Sniffer for analysis, or viewed via the menu-driven user interface. When viewed from the menu-driven user interface, the twelve most recent LMI messages are displayed via the LMI Trace Log.

- **Integral Modem.** Provides an internal 14.4 Kbps modem to support dialing in to the unit for out-of-band management and automatic dialing out of SNMP traps.

- **Modem PassThru.** Provides access to another device's VT100-compatible user interface over a dial connection. When this feature is enabled, a logical connection between the unit's modem and COM ports is created, allowing access to a collocated device's serial port via the FrameSaver unit's internal modem. This feature is sometimes referred to as the Router Assist feature.

- **Configurable FTP Transfer Rate.** Allows you to control the transmit rate when downloading firmware into the FrameSaver unit and uploading user history statistics to an NMS (Network Management System) via the COM port connection or a management PVC so the data can be transferred as a background task using the standard File Transfer Protocol (FTP) over extended periods of time using low bandwidth.

- **RMON User History Performance Statistics via SNMP Polling.** Provides access to the physical interface and basic frame relay performance statistics by polling the FrameSaver unit using SNMP (Simple Network Management Protocol). These statistics are available real-time via the Enterprise MIB and historically as an RMON2 User History object.

- **Frame Relay Traffic Policing.** Ensures proper alignment and correlation of CIR (Committed Information Rate) values between the FrameSaver unit and the network switch. When this feature is enabled, the unit can enforce CIR and EIR (Excess Information Rate), marking frames that exceed CIR as DE (Discard Eligible) using the same method used by the switch.

- **Service Provider Support.** Provides information and tools useful to network service providers, which includes the following:

  — IP Routing Table – Shows the IP routing table for the FrameSaver unit, with network as well as host routes, the number of hops to the destination, the method by which the route was added to the table, the interface used to get to the destination, and how long the route has been in existence.

  — Trap Event Log – Displays the SNMP (Simple Network Management Protocol) trap event log for the FrameSaver unit from the menu-driven user interface, with the most recent events first, keeping a running total for all trap events stored, the amount of time since the event was logged, plus a description of the trap.

  — Troubleshooting PVC – Provides a dedicated troubleshooting management link that helps service providers isolate problems within their network.

- **ATM VPI/VCI and DLCI Correlation.** For networks with both ATM and frame relay-access endpoints, allows the FrameSaver unit to report the originating Virtual Path and Channel Identifier (VPI/VCI) in the far-end ATM-access endpoint where the local DLCI is mapped so they can be correlated for OpenLane SLV reports.

- **Dual Flash Memory.** Allows software upgrades while the unit is up and running. Two software loads can be stored and implemented at the user's discretion.

- **DSX-1 Drop/Insert Port.** Allows DTEs/PBXs that support the DS1 signal format to share the T1 network with other high-speed equipment so that voice traffic can share the same local access circuit as the frame relay data.
- **Back-to-Back Operation.** Allows two FrameSaver devices to be connected via a leased-line network or simulation so a point-to-point configuration can be implemented.
- **Enhanced Ping Operation.** FrameSaver devices can check connectivity and roundtrip response time to any remote device in either direction, via the FrameSaver internal management network or the data path.
- **Payload Management.** Any standard, non-management DLCI can be designated as payload managed, providing management directly from a user data PVC, and support for Telnet, ping, SNMP, and FTP.
- **Optional ISDN Backup.** FrameSaver SLV 9126 and 9126-II CSU/DSUs can be equipped with a BRI DBM, which supports up to two channels. The channels may have different destinations. The DBM may be field-installed in the FrameSaver SLV 9126 CSU/DSU, and must be factory-installed in the 9126-II CSU/DSU.

  FrameSaver SLV 9128-II 1-slot units can be equipped with a PRI DBM, which supports up to 23 B-channels, or a BRI DBM. Carrier-mounted FrameSaver SLV 9128-II NAMs support a PRI DBM only.

  When an ISDN BRI or PRI DBM (Basic Rate Interface or Primary Rate Interface Dial Backup Module) is installed, the following ISDN backup features are provided:

  — Provides automatic dial backup through the ISDN for data when primary frame relay network or access line failures occur, then automatically restores data to the primary route when service returns to normal. Backup is supported regardless of whether or not Caller ID is provisioned on the ISDN circuit. A secondary backup phone number is also available to call when a backup link cannot be established with the primary backup site.

  — Supports simultaneous origination, answering, or origination and answering backup calls, as needed, based upon how the ISDN Link Profile is set up. This feature is also known as peer-to-peer calling.

  — Provides automatic configuration of an alternate route and DLCI for automatically created PVCs at either the remote site or central site based upon the learned far-end DLCI number. When the automatic backup feature is enabled, backup and restoration occur automatically.

  — Provides backup timers that can be configured to better control the amount of time required before backup is initiated, when a backup call will be terminated once the failure condition clears, and a delay before normal service is restored. These features are useful during periods of frequent service disruption.

  In addition, round trip latency thresholds can be configured that will initiate backup when configured thresholds are exceeded.

  — Supports backup call groups, where redundant PVCs can be assigned to a specified call group. Using this feature, the unit only goes into backup when *all* PVCs in the group are down, and it returns to normal service as soon as *one* PVC in the group is operational again. This feature is useful when multiple PVCs are going to redundant central sites.

- When the SLV Sample Interval is set to 10 seconds, provides advance detection of network problems before a DLCI Down indication is received, to minimize data loss.
- Provides customer premises equipment (CPE) with a Backward Explicit Congestion Notification (BECN) when backup bandwidth is not sufficient for the traffic, allowing the CPE time to slow traffic to the ISDN before the network starts discarding data.
- Supports Frame Relay Forum Multilink Frame Relay Implementation Agreement – FRF.15 so backup bandwidth can be increased by aggregating multiple B-channels over the ISDN link.
- Supports collection of call and call attempt statistical information that can be viewed from the menu-driven user interface or via SNMP, and supports alarm generation and call security, as well.
- Provides test call capability on ISDN backup links so ISDN and DBM function can be verified before there is an actual primary link failure and switched over to the backup link. Periodic tests are recommended, which can be performed from the menu-driven user interface, or through SNMP commands. Multiple Last Cause Values are also provided to assist in troubleshooting ISDN problems.

Additional FrameSaver SLV 9126-II and 9128-II Features

- **Ethernet Interface.** FrameSaver SLV 9126-II Routers and 9126-II and 9128-II CSU/DSUs units have a 10/100 BaseT Ethernet LAN interface for management, with automatic sensing of the operation rate of 10 Mb or 100 Mb, conforming to ANSI/IEEE 802.3.

Additional FrameSaver SLV 9128-II Features

The following features are unique to FrameSaver SLV 9128-II units:

- **Multiple Data Ports.** Provides two data ports instead of one, which have standard connectors so no special-order cables are required.
- **Carrier-Mounted Models.** For customers with high-density requirements, FrameSaver SLV 9128s and 9128-IIs can be ordered as multislot units, called Network Access Modules (NAMs), for insertion in the 14-slot 9000 Series Access Carrier.

FrameSaver SLM Feature Set

A FrameSaver SLV unit with the advanced SLM feature set provides the following features in addition to those provided with the basic set:

- **TruePut™ Technology.** Using Frame Delivery Ratios (FDR) and Data Delivery Ratios (DDR), throughput (within and above CIR, as well as between CIR and EIR, and above EIR) can be measured precisely, eliminating inaccuracies due to averaging.
- **Intelligent Service Level Verification.** Provides accurate throughput, latency, and availability measurements to determine network performance and whether service level agreements (SLAs) are being met, along with SLA reporting.
- **RMON Alarms and Configurable Alarm Thresholds.** Provides the ability to change SLA parameter and RMON alarm thresholds via the OpenLane system to correct them in real-time, before the SLA is violated.
- **Multiplexed Customer PVCs.** Provides a method of multiplexing customer management data and user data with network management data transparently over a single PVC when FrameSaver devices are at each end of the circuit.
- **FTP User History Poller.** Provides a bulk collector using FTP through the OpenLane system that generates a file for data at the time that data is uploaded using FTP.
- **Network User History Synchronization.** Allows correlation of RMON2 User History statistics among all SLV devices in a network. Using a central clock, called the network reference time, all SLV device user history statistics are synchronized across the network, further enhancing the accuracy of OpenLane SLV reports.
- **RMON-Based User History Statistics Gathering.** Provides everything needed to monitor network service levels, plus throughput with accurate data delivery, network latency, and LMI and PVC availability. Continuous roundtrip latency testing and reporting, as well as CIR to transmitted and received data performance statistics, are included.

  In addition, port bursting statistics are kept for all frame relay links for accurate calculation of utilization.

OpenLane SLM System

Being standards-based, the OpenLane SLM (Service Level Management) system can be used with other management applications like HP OpenView or IBM's NetView. OpenLane includes HP OpenView adapters for integrating OpenLane features with the OpenView Web interface.

Being Web-based, the OpenLane system provides Web access to the data contained in the database to provide anytime, anywhere access to this information via a Web browser.

Some of the OpenLane system's features include:

- Real-time performance graphs provide exact performance measurement details (not averages, which can skew performance results) of service level agreement (SLA) parameters.

  Port bursting and EIR (Excess Information Rate) performance monitoring graphs are available when the software release for the OpenLane SLM system is Release 5.2, or later.

- Historical SLV graphs provide service level management historical reports so frame relay SLAs can be verified.

- Diagnostic troubleshooting provides an easy-to-use tool for performing tests, which include end-to-end, PVC loopback, connectivity, and physical interface tests.

  For units with ISDN backup capability, provides ISDN physical interface and PVC testing when the software release for the OpenLane SLM system is Release 5.2, or later.

- Basic configuration allows you to configure FrameSaver devices. Network DLCI Circuit IDs can also be assigned.

- Automatic SLV device and PVC discovery allows all SLV devices with their SLV Delivery Ratio configuration option enabled to be discovered automatically, along with their PVCs.

- A FrameSaver unit can be reset from the OpenLane system.

- Firmware downloading provides an easy-to-use tool for downloading to an entire network or a portion of the network.

- On-demand polling of FrameSaver devices, and SNMP polling and reporting are available.

- The maintenance scheduling feature allows for the scheduling of multiple periodic maintenance periods, and provides a record of all scheduled maintenance periods – past, present, and future.

NetScout Manager Plus and NetScout Probes

Provides complete LAN and WAN traffic analysis and monitoring functions for FrameSaver devices.

The following features are supported using this application:

- Thresholds for RMON 1 (Remote Monitoring, Version 1) alarms and events can be configured.

- Performance monitoring can be performed using collected RMON 2 (Version 2) data. NetScout Manager Plus's Protocol Directory and Distribution functionality allows FrameSaver devices to measure up to eleven network-layer protocols and report the amount of traffic generated by each. Its IP Top Talkers and Listeners reporting identifies the devices using network bandwidth for traffic and protocol analysis, identifying the network's top six users. In addition, it collects performance statistics from FrameSaver devices. Up to 900 samples can be stored in 15-minute buckets, with 96 buckets in a 24-hour period, for up to five days worth of data.

- Optional standalone NetScout Probes can be used with FrameSaver devices at sites where full 7-layer monitoring, an unlimited number of protocols, and advanced frame capture and decode capabilities are desired.

User Interface and Basic Operation

2

This chapter contains information about how to access, use, and navigate the menu-driven user interface and the Router's Command Line Interface (CLI). It includes the following:

Logging On

Start a session using one of the following methods:

- Telnet session via:
  - An in-band management channel through the frame relay network.
  - A local in-band management channel configured on the DTE port between the FrameSaver unit and the router.
- Dial-in connection using the internal modem.
- Direct terminal connection over the COM port.

When logging on, the User Interface Idle screen appears.

- If no security was set up or security was disabled, the Main Menu screen appears (see *Main Menu* on page 2-4). You can begin your session.
- If security was set up and is enabled, you are prompted for a login. Enter your login ID and password.

When the user interface has been idle, a session is automatically ended and the screen goes blank when the unit times out. Press Enter to reactivate the interface.

▶ Procedure

To log in when security is being enforced:

1. Type your assigned Login ID and press Enter.
2. Type your Password and press Enter.
   - Valid characters – All printable ASCII characters
   - Number of characters – Up to 10 characters can be entered in the Login ID and Password fields
   - Case-sensitive – Yes

   An asterisk (*) appears in the password field for each character entered.

If your login was . . .	Then the . . .
Valid	Main Menu appears. Begin your session. **NOTE:** If your login is valid, but access is denied, there are two currently active sessions.
Invalid	Message, **`Invalid Password`**, appears on line 24, and the Login screen is redisplayed. After three unsuccessful attempts: ■ A Telnet session is closed. ■ The User Interface Idle screen appears for a directly connected terminal. ■ The internal modem connection is disconnected. ■ An SNMP trap is generated. Access is denied. See your system administrator to verify your login (Login ID/Password combination).

FrameSaver units support two sessions simultaneously. If two sessions are currently active, wait and try again.

- If two sessions are currently active and you are attempting to access the unit through Telnet, the local Telnet client process returns a **`Connection refused:`** message at the bottom of the screen.
- If two sessions are currently active and you are attempting to access the unit over the COM port or modem port, not via Telnet, the User Interface Already In Use screen is redisplayed. In addition, the type of connection (Telnet Connection, Direct COM Port Connection, or Direct Modem Port Connection) for each current user is identified, along with the user's login ID.

▶ Procedure

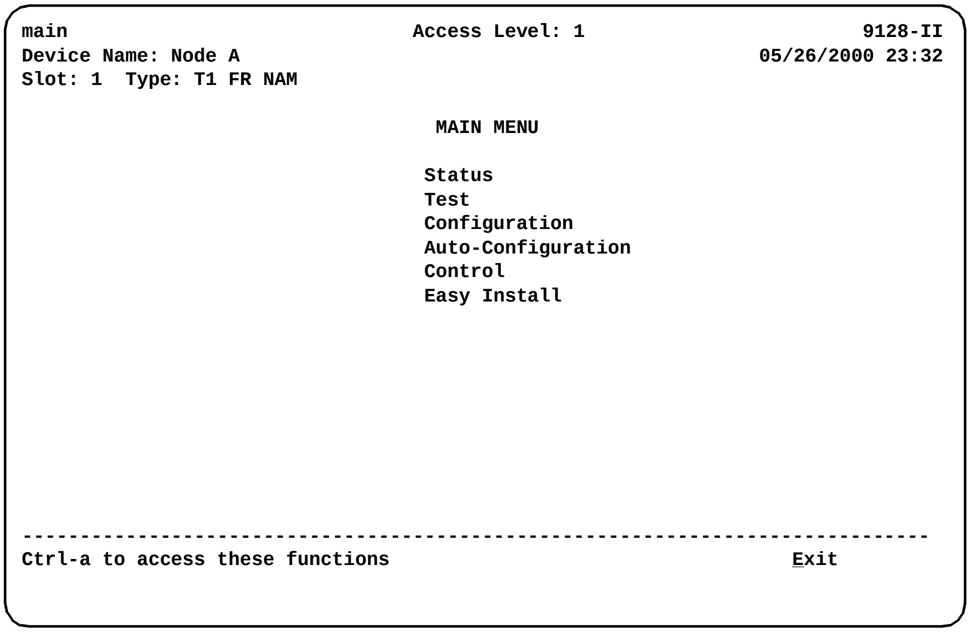
To end the session:

1. Press Ctrl-a to switch to the function keys area of the screen.
2. Type **e** (Exit) and press Enter.
   - — For a terminal-connected to the COM port, the session is ended.
   - — For a terminal-connected to the modem port, the session is ended and the modem is disconnected.
   - — For a Telnet connection, the session is closed and, if no other Telnet or FTP session is occurring over the connection, the modem is disconnected.

If ending a session from the Configuration branch, see *Saving Configuration Options* in Chapter 3, *Configuration Procedures*.

Main Menu

Entry to all of the FrameSaver unit’s tasks begins at the Main Menu, which has six menus or branches. The Access Level at the top of the screen only appears when security has been set up.



```
main                              Access Level: 1                     9128-II
Device Name: Node A                                          05/26/2000 23:32
Slot: 1  Type: T1 FR NAM

                                    MAIN MENU

                                   Status
                                   Test
                                   Configuration
                                   Auto-Configuration
                                   Control
                                   Easy Install









------------------------------------------------------------------------------
Ctrl-a to access these functions                                 Exit
```

Select . . .	To . . .
Status	View diagnostic tests, interfaces, PVC connections, and statistics. You can also display LEDs and FrameSaver unit identity information.
Test	Select and cancel test for the FrameSaver unit’s interfaces.
Configuration	Display and edit the configuration options.
Auto-Configuration	Configure basic access unit setup automatically based upon a selected application. You can also automatically populate network and (for CSU/DSUs) data port DLCI configuration options with numeric settings.
Control	Control the asynchronous user interface for call directories, device naming, login administration, and selecting software releases. You can also initiate a power-on reset of the FrameSaver unit.
Easy Install	Configure minimal options for a quick installation.

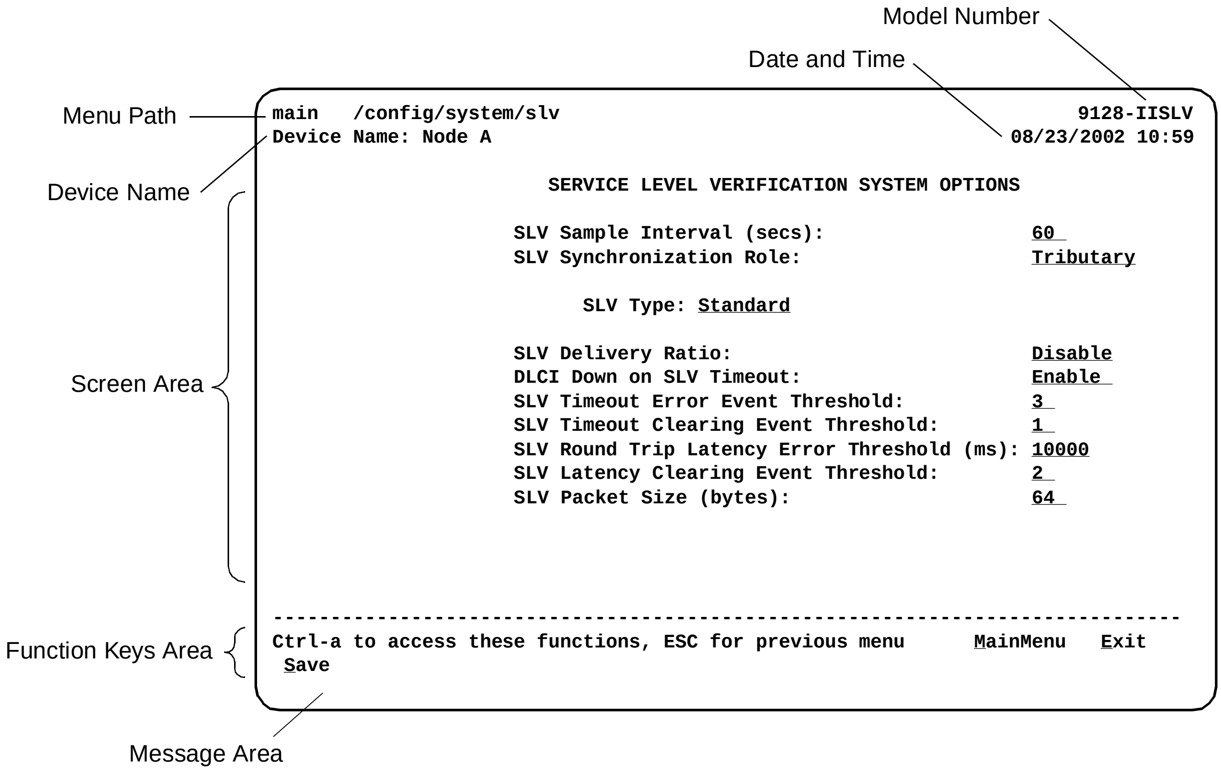
See Appendix A, *Menu Hierarchy*, for a pictorial view of the menu hierarchy, which represents the organization of the FrameSaver unit’s menus and screens.

Screen Work Areas

There are two user work areas:

- **Screen area** – Where you input information into fields.
- **Function keys area** – Where you perform specific screen functions.

Below is a sample configuration screen.



```
main   /config/system/slv                                               9128-IISLV
Device Name: Node A                                               08/23/2002 10:59

                        SERVICE LEVEL VERIFICATION SYSTEM OPTIONS

                     SLV Sample Interval (secs):                  60
                     SLV Synchronization Role:                    Tributary

                           SLV Type: Standard

                     SLV Delivery Ratio:                          Disable
                     DLCI Down on SLV Timeout:                    Enable
                     SLV Timeout Error Event Threshold:           3
                     SLV Timeout Clearing Event Threshold:        1
                     SLV Round Trip Latency Error Threshold (ms): 10000
                     SLV Latency Clearing Event Threshold:        2
                     SLV Packet Size (bytes):                     64




-------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save
```

Screen Format	Description
Menu Path	Menu selections made to reach the current screen.
Device Name	Customer-assigned identification of the FrameSaver unit.
9126, 9126-SLV, 9126-IISLV, 9126-IIR, 9126-IIRSLV, 9128-II, or 9128-IISLV	FrameSaver unit's model number.
Screen Area	Selection, display, and input fields for monitoring and maintaining the FrameSaver unit.
Function Keys Area	Specific functions that can be performed by pressing a specified key, then pressing Enter.
Message Area	System-related information and valid settings for input fields are in the lower left corner. System and Test Status messages are in the lower right corner.

Navigating the Screens

You can navigate the screens by:

- Using keyboard keys.
- Switching between the two screen work areas using function keys.

Keyboard Keys

Use the following keyboard keys to navigate within the screen area:

Press . . .	To . . .
Ctrl-a	Move cursor between the screen area and the screen function keys area.
Esc	Return to the previous screen.
Right Arrow (on same screen row), or Tab (on any screen row)	Move cursor to the next field.
Left Arrow (on same screen row), or Ctrl-k	Move cursor to the previous field.
Backspace	Move cursor one position to the left or to the last character of the previous field.
Spacebar	Select the next valid value for the field.
Delete (Del)	Delete character that the cursor is on.
Up Arrow or Ctrl-u	Move cursor up one field within a column on the same screen.
Down Arrow or Ctrl-d	Move cursor down one field within a column on the same screen.
Right Arrow or Ctrl-f	Move cursor one character to the right if in edit mode.
Left Arrow or Ctrl-b	Move cursor one character to the left if in edit mode.
Ctrl-l	Redraw the screen display, clearing information typed in but not yet entered.
Enter (Return)	Accept entry or, when pressed before entering data or after entering invalid data, display valid options on the last row of the screen.

Function Keys

All function keys (located in the lower part of the screen; see the example in *Screen Work Areas* on page 2-5) operate the same way throughout the screens. They are not case-sensitive, so upper- or lowercase letters can be used interchangeably.

These keys use the following conventions:

Select . . .	For the screen function . . .	And press Enter to . . .
M or m	MainMenu	Return to the Main Menu screen.
E or e	Exit	Terminate the asynchronous terminal session.
N or n	New	Enter new data.
O or o	Modify	Modify existing data.
L or l	Delete	Delete data.
S or s	Save	Save information.
R or r	Refresh	Update screen with current information.
C or c	ClrStats	Clear network performance statistics and refresh the screen. Variations include: ■ ClrSLV&DLCIStats for clearing SLV and DLCI statistics. ■ ClrLinkStats for clearing frame relay link statistics. ■ ClrDBMStats for clearing DBM call statistics.
U or u	PgUp	Display the previous page.
D or d	PgDn	Display the next page.

Selecting from a Menu

▶ Procedure

To select from a menu:

1. Tab or press the down arrow key to position the cursor on a menu selection, or press the up arrow key to move the cursor to the bottom of the menu list.

   Each menu selection is highlighted as you press the key to move the cursor from position to position.

2. Press Enter. The selected menu or screen appears.

▶ Procedure

To return to a previous screen, press the Escape (Esc) key until you reach the desired screen.

Switching Between Screen Areas

Use Ctrl-a to switch between screen areas (see the example in *Main Menu* on page 2-4).

▶ Procedure

To switch to the function keys area:

1. Press Ctrl-a to switch from the screen area to the function keys area.
2. Select either the function's designated (underlined) character or Tab to the desired function key.
3. Press Enter. The function is performed.

To return to the screen area, press Ctrl-a again.

Selecting a Field

Once you reach the desired menu or screen, select a field to view or change, or issue a command.

Press the Tab or right arrow key to move the cursor from one field to another. The current setting or value appears to the right of the field.

Entering Information

You can enter information in one of three ways. Select the field, then:

- Manually type in (enter) the field value or command.

  Example:
  Entering **bjk** as a user's Login ID on the Administer Logins screen (from the Control menu/branch).

- Type in (enter) the first letter(s) of a field value or command, using the unit's character-matching feature.

  Example:
  When configuring a port's physical characteristics with the Port (DTE) Initiated Loopbacks configuration option/field selected (possible settings include Disable, Local, DTPLB, DCLB, and Both), entering **d** or **D** displays the first value starting with d – Disable. In this example, entering **dt** or **DT** would display DTPLB as the selection.

- Switch to the function keys area and select or enter a designated function key.

  Example:
  To save a configuration option change, select Save. S or s is the designated function key.

If a field is blank and the Message area displays valid selections, press the spacebar; the first valid setting for the field appears. Continue pressing the spacebar to scroll through other possible settings.

Screen Contents

What appears on the screens depends on:

- **Current configuration** – How your network is currently configured.
- **Security access level** – The security level set by the system administrator for each user.
- **Data selection criteria** – What you entered in previous screens.

Navigating the Router's CLI

Access the FrameSaver DSL Router's Command Line Interface by pressing the Shift-r function key from the Main Menu. There is no need to press Ctrl-a first to access the function keys area of the screen.

Once the CLI is accessed, you can use keyboard keys to navigate within the interface. Using the router's CLI, you can display and edit router configuration settings, view router status, and access router tests.

For details of all CLI commands and the conventions used when entering commands, see Appendix C, *Router CLI Commands, Codes, and Designations.* For a summary of abbreviated (minimal) command entries and their default settings, see Appendix D, *Router Command Line Summaries and Shortcuts.*

CLI Keyboard Keys

Use the following keyboard keys to navigate within the router's CLI. Most terminal emulation programs use these same keys.

Press . . .	**To . . .**
Enter (Return)	Accept the current command line input.
Ctrl-c	■ Clear the current command line entry. ■ Abort a command line prompt without answering. ■ Exit a command in progress.
Ctrl-z	Exit Configuration mode and returns to Standard mode. A prompt appears to save any unsaved changes.
Backspace	Erase the character to the left of the cursor.
Delete	Erase the character the cursor is on.
Down Arrow	Recall command line history buffer with the most recent command displaying first. Buffer contains ten lines of history.
Up Arrow	Scroll to the last valid command for editing.
Right Arrow	Move the cursor one position to the right.
Left Arrow	Move the cursor one position to the left.
q (or any key but Spacebar or Enter/Return)	Abort a Move display and return to the command line prompt.

Configuration Procedures

3

This chapter includes the following:

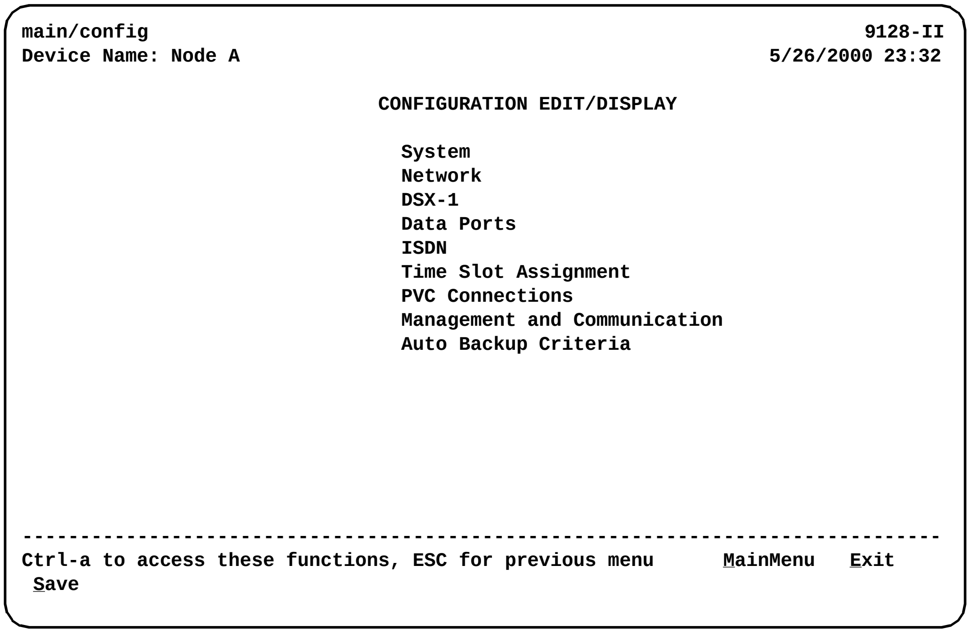
- *Basic Configuration*
  - — *Configuration Option Areas*
  - — *Accessing and Displaying Configuration Options*
  - — *Changing Configuration Options*
  - — *Saving Configuration Options*

Basic Configuration

Configuration option settings determine how the FrameSaver unit operates. Use the FrameSaver unit's Configuration Edit/Display menu to display or change configuration option settings.

The Configuration Edit/Display menu shown below is for a FrameSaver SLV 9128-II with the optional ISDN backup feature.

Configuration Menu



```
main/config                                                                 9128-II
Device Name: Node A                                                5/26/2000 23:32

                               CONFIGURATION EDIT/DISPLAY

                                 System
                                 Network
                                 DSX-1
                                 Data Ports
                                 ISDN
                                 Time Slot Assignment
                                 PVC Connections
                                 Management and Communication
                                 Auto Backup Criteria








--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save
```

Changing an Auto-Configuration setting can also change the FrameSaver unit's configuration. See *Setting Up Auto-Configuration* in Chapter 4, *Configuration Options,* for additional information.

Configuration Option Areas

The FrameSaver unit arrives with configured factory default settings, which are located in the Factory Default Configuration option area. You can find the default settings for configuration options in the:

- *FrameSaver SLV 9126 and 9126-II Quick Reference*, *FrameSaver SLV 9128/9128-II Quick Reference*, or *FrameSaver SLV 9126-II Router Quick Reference*
- *Configuration Option Tables* in Chapter 4, *Configuration Options*

If the factory default settings do not support your network's configuration, you can customize the configuration options to better suit your application.

Four configuration option storage areas are available.

Configuration Option Area	Description
Current Configuration	The currently active set of configuration options.
Customer Configuration	An alternate set of configuration options that you can set up and store for future use.
Scratchpad Configuration	An alternate configuration area for temporary use. The Scratchpad configuration is reset to the factory default settings when the unit is powered off and on.
Default Factory Configuration	A read-only configuration area containing the factory default set of configuration options. You can load and edit default factory configuration settings, but you can save changes only to the Current, Customer, or Scratchpad configuration option areas.

Accessing and Displaying Configuration Options

To access and display configuration options, load (copy) the applicable configuration option set into the edit area.

▶ Procedure

To load a set of configuration options for editing:

1. From the Main Menu, press the down arrow key so the cursor is on Configuration.

2. Press Enter to display the Configuration menu. The **Load Configuration From:** menu appears.

   NOTE:

   Loading a configuration with many DLCIs from a unit's Customer or Scratchpad configuration option area may take time. Allow a minute or more for the file to be loaded.

3. Select the configuration option area from which you want to load configuration options and press Enter (Current Configuration, Customer Configuration, Scratchpad Configuration, or Default Factory Configuration).

   The selected set of configuration options is loaded into the configuration edit area and the **Configuration Edit/Display** menu appears.

This sequence of steps would be shown as the menu selection sequence:

Main Menu→Configuration

Changing Configuration Options

▶ Procedure

To change configuration option settings:

1. From the **Configuration Edit/Display** menu, select a set of configuration options and press Enter.

   For example:
   Configuration→PVC Connections

2. Select the configuration options that are applicable to your network, and make appropriate changes to the setting(s). See Chapter 2, *User Interface and Basic Operation*, for additional information.

   When creating new PVC connections or management PVCs, some configuration options will be blank. For a valid setting to appear, Tab to the configuration option and press the spacebar.

3. Repeat Steps 1 and 2 until all changes are complete.

NOTES:

— Only Security Access Level 1 users can change configuration options.

— Security Access Level 2 users can only view configuration options and run tests.

— Security Access Level 3 users can only view configuration options; they cannot change configuration options or run tests.

Saving Configuration Options

When changes to the configuration options are complete, use the Save function key to save your changes to either the Current, Customer, or Scratchpad configuration areas.

NOTE:

When changing settings, you must Save for changes to take effect.

▶ Procedure

To save the configuration option changes:

1. Press Ctrl-a to switch to the function key area at the bottom of the screen.
2. Type **s** or **S** to select the Save function and press Enter.

   The **Save Configuration To:** screen appears.

   NOTE:

   If you try to exit the Configuration menu without saving changes, a Save Configuration screen appears requiring a Yes or No response.

   — If you select No, the Main Menu screen reappears and the changes are not saved.

   — If you select Yes, the **Save Configuration To:** screen appears.

3. Select the configuration option area to which you want to save your changes (normally the Current Configuration) and press Enter.

   When Save is complete, **`Command Complete`** appears in the message area at the bottom of the screen.

   NOTE:

   There are other methods of changing configurations, like SNMP and Auto-Configuration. Since multiple sessions can be active at the same time, the last change made overwrites any previous or current changes being made. For instance:

   — Saving your configuration changes would cause configuration changes made via another method to be lost.

   — If you are making changes and someone else makes changes and saves them, your changes would be lost.

Configuration Options

4

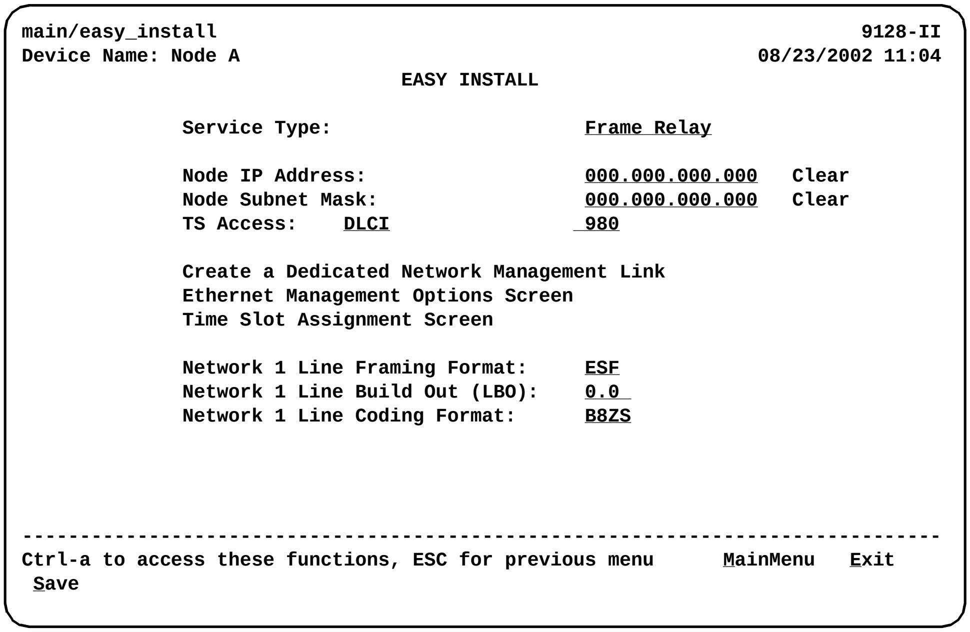
This chapter includes the following:

Using the Easy Install Feature

The Easy Install feature provides a straight-forward installation menu that requires minimal configuration to get the FrameSaver unit up and running quickly, and to set up remote configuration and management via Telnet access from the NOC (Network Operations Center).

Main Menu→Easy Install

Easy Install Screen Example*



```
main/easy_install                                                       9128-II
Device Name: Node A                                            08/23/2002 11:04
                                 EASY INSTALL

              Service Type:                      Frame Relay

              Node IP Address:                   000.000.000.000   Clear
              Node Subnet Mask:                  000.000.000.000   Clear
              TS Access:    DLCI                  980

              Create a Dedicated Network Management Link
              Ethernet Management Options Screen
              Time Slot Assignment Screen

              Network 1 Line Framing Format:     ESF
              Network 1 Line Build Out (LBO):    0.0
              Network 1 Line Coding Format:      B8ZS




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save
```

* The Ethernet Management Options Screen applies to the 9126-II (both CSU/DSU and Router) and 9128-II. For the Model 9126, DS0 Base Rate (Kbps) appears after the Network 1 Line Coding Format option.

To remotely access the FrameSaver unit in Frame Relay mode, use the Dedicated Network Management Link that was created during installation, using the Node IP Address that was entered for the unit.

See the *FrameSaver SLV 9126-II 1-Slot Unit Installation Instructions*, the *FrameSaver SLV 9128/9128-II 1-Slot Unit Installation Instructions*, or the *FrameSaver SLV 9128/9128-II Network Access Module (NAM) Installation Instructions* for additional information and installation procedures.

Using RIP with FrameSaver SLV CSU/DSUs

Using the system's standard Routing Information Protocol (RIP) feature, routing information is passed to the router over the management PVC, so the router can learn routes to FrameSaver SLV and FLEX devices. Node IP information should be set up (see *Configuring Node IP Information* on page 4-74).

▶ Procedure

To set up your router and FrameSaver SLV CSU/DSU so that the router can learn routes to FrameSaver devices:

1. Configure the router to receive RIP.

   For example, if using a Cisco router, you would use the commands **`config-t`**, **`router RIP`**, **`int serialx`**, **`IP RIP Receive version 1`**, then **`ctl-z WR`**.

2. Create a Standard DLCI for the user data port.

   Configuration→Data Ports→DLCI Records

3. Create a Management PVC using the user data port DLCI just configured.

   Configuration→Management and Communication→Management PVCs

4. Set Primary Link RIP to Standard_Out, and Save the configuration.

Refer to Table 4-14, DLCI Record Options, and Table 4-18, Management PVC Options, for configuration information.

Entering System Information and Setting the System Clock

Select System Information to set up or display the general SNMP name for the unit, its location, and a contact for the unit, as well as to set the system clock.

Main Menu→Control→System Information

The following information is available for viewing. Save any entries or changes.

If the selection is . . .	Enter the . . .
Device Name	Unique name for device identification of up to 20 characters.
System Name	SNMP system name; can be up to 255 characters.
System Location	System's physical location; can be up to 255 characters.
System Contact	Name and how to contact the system person; can be up to 255 characters.
Date	Current date in the month/day/year format (mm/dd/yyyy).
Time	Current time in the hours:minutes format (hh:mm).

NOTE:

To clear existing information, place the cursor in the Clear field (Tab to the Clear field) and press Enter.

See Chapter 6, *Security and Logins*, to set up and administer logins.

Setting Up the Modem

The unit has an internal modem for dial-in access to the menu-driven user interface, as well as dial-out capability when an SNMP trap is generated. When the modem will be used to dial out, Modem Directory phone numbers need to be set up. Otherwise, simply configure or change dial-in access to the unit.

The modem port is already configured for connection to an asynchronous terminal and dial-in access, with Port Use set to Terminal. However, additional changes may be needed (see Table 4-25, Modem Port Options).

Main Menu→Configuration→Management and Communication→ Modem Port

For dial-in access to the menu-driven user interface via Telnet, make sure Port Use is set to Net Link, the IP address and subnet mask are entered if they are different from the node's, and that the Link Protocol is correct.

For dial-in access to the router connected to the unit's COM port, make sure the Communication Port's Port Use option is set to Modem PassThru.

See *Setting Up Call Directories for Trap Dial-Out* on page 4-6, when trap dial-out is desired. See *Setting Up to Use the Modem PassThru Feature* on page 4-7, if this feature is desired. See *Limiting Dial-In Access via the Modem Port* in Chapter 6, *Security and Logins*, for additional information.

Setting Up Call Directories for Trap Dial-Out

▶ Procedure

1. Set up directory phone numbers.

   Main Menu→Control→Modem Call Directories

2. Select Directory Number A (for Alarm).

3. Enter the phone number(s).

Valid characters include . . .	For . . .
ASCII text	Entering the phone number.
Space, underscore (_), and dash (–)	Readability characters.
Comma (,)	Readability character for a 2-second pause.
B	Blind dialing.
P	Pulse dialing, unless B is specified.
T	Tone dialing, unless B is specified.
W	Wait for dial tone.

4. Save the phone number(s).

Setting Up to Use the Modem PassThru Feature

Dial-in access to the router is possible via the Modem PassThru feature, also known as the Router Assist feature. The FrameSaver unit's COM port must be connected to the router's auxiliary (AUX) or console port, and the COM port must be configured for this use.

When this feature is set up and active, a logical connection between the unit's modem and COM ports is made, and data received over the modem port is transmitted out the COM port to the router's AUX or console port. When an escape sequence (minus, minus, minus, with a minimum of 50 ms between each) is detected, the FrameSaver unit switches back to normal user interface operation.

See *COM Port-to-Router Cables* in Appendix E, *Connectors, Cables, and Pin Assignments*, for cable information.

▶ Procedure

1. Configure the COM port to use Modem PassThru.

   Main Menu→Configuration→Management and Communication→ Communication Port

2. Set Port Use to Modem PassThru.

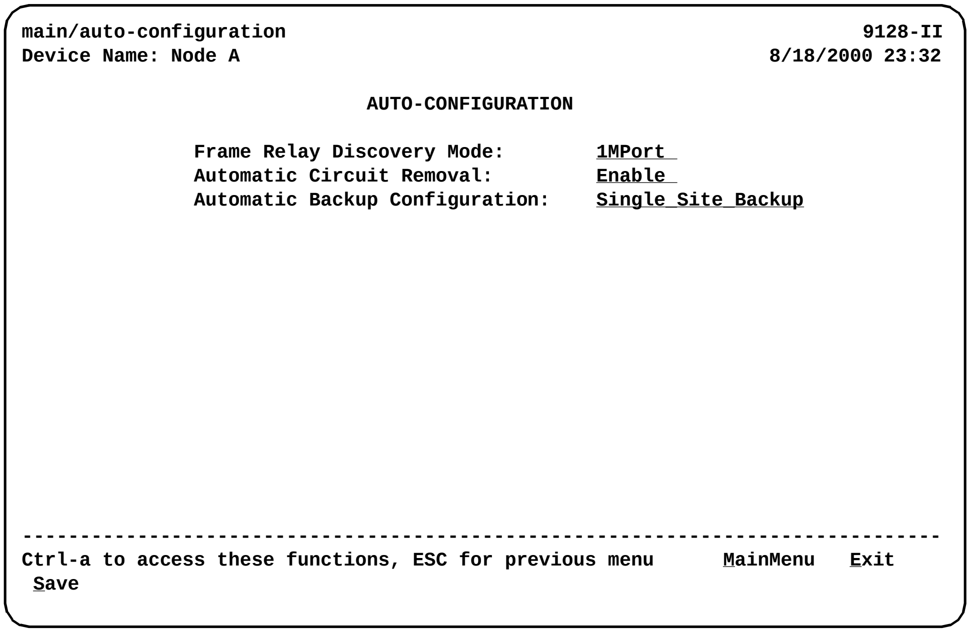
3. Save the configuration.

Setting Up Auto-Configuration

The auto-configuration feature allows you to select a method of automatic configuration and connection of DLCIs within the FrameSaver unit, as well as to automatically remove DLCIs and connections that are no longer supported by the network service provider.

Main Menu→Auto-Configuration

Auto-Configuration Screen Example



```
main/auto-configuration                                                   9128-II
Device Name: Node A                                               8/18/2000 23:32

                                AUTO-CONFIGURATION

              Frame Relay Discovery Mode:        1MPort
              Automatic Circuit Removal:         Enable
              Automatic Backup Configuration:    Single Site Backup















--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save
```

This feature also maintains associated DLCI option settings when Standard LMI is used on the network interface.

If an ISDN DBM is not installed, Automatic Backup Configuration does not appear (see *Setting Up Automatic Backup Configuration* on page 4-13) for additional information).

Selecting a Frame Relay Discovery Mode

When a Frame Relay Discovery Mode is active, the FrameSaver unit “discovers” network DLCIs from the network LMI status response message. It configures a network DLCI and a user data port DLCI, and automatically connects them to create a PVC.

Main Menu→Auto-Configuration→Frame Relay Discovery Mode

Automatically configured network DLCIs are multiplexed, and each automatically configured port DLCI carries the same DLCI Number as its corresponding network DLCI. These are the same DLCI numbers that would have been available had the FrameSaver unit not been inserted in the link, between your equipment and the network.

NOTE:

A local Management PVC (e.g., the PVC between the router and the FrameSaver unit’s user data port) must be configured manually.

The following will occur when a Frame Relay Discovery Mode is selected:

Discovery Mode	Configuration Description
1MPort	■ Auto-configuration is enabled on Port-1. ■ A management DLCI is configured. ■ A multiplexed network DLCI containing two embedded DLCIs (EDLCIs) is configured for Port-1 user data and management data. ■ A PVC connection is configured between the network and port DLCIs.
1Port	■ Auto-configuration is enabled on Port-1. ■ No management DLCI is configured. ■ A multiplexed network DLCI is configured for Port-1 user data. ■ A PVC connection is configured between the network and port DLCIs.
1PPort	■ Auto-Configuration is enabled on Port-1. ■ A Port-1 DLCI is created for each network DLCI and automatically cross-connected to it. ■ Payload management is configured for the network DLCI and assigned the Node IP Address.
2MPorts *(only applies to models with multiple data ports)*	■ Auto-configuration is enabled on both Port-1 and Port-2. ■ A multiplexed network DLCI containing three EDLCIs is configured for Port-1 customer data, Port-2 customer data, and management data. ■ PVC connections are configured between the network and port DLCIs. ■ A management PVC is configured on the network interface.

Discovery Mode	Configuration Description
NetOnly	■ Auto-configuration of a network DLCI only; no Port-1 or PVC connections are configured. ■ No Port-1, PVC connection, or management DLCI is configured.
Disable	■ No frame relay discovery or automatic configuration takes place. The FrameSaver unit will be configured manually.

NOTE:

If the default setting (1MPort or 1PPort) is not the setting required for your application, change the Frame Relay Discovery Mode **before** connecting the network cable or editing discovered option settings. Otherwise, the FrameSaver unit will start discovering DLCIs as soon as it powers up.

If this occurs, you can recover by deleting the discovered DLCIs. If only a local management PVC between the router and the FrameSaver unit has been configured, simply select the desired Frame Relay Discovery Mode and Save the change.

The default discovery mode, depending on model, is 1MPort or 1PPort.

When 1MPort mode is active, the unit creates for each DLCI discovered on the network a multiplexed network interface DLCI (which contains two EDLCIs: one for Port-1 data and the other for management), a standard Port-1 DLCI (with the same number as the network interface DLCI), and a Management PVC, then cross-connects them. When LMI is active on the network interface and PVC status information (with provisioned DLCI numbers) is next received from the network, the unit automatically saves the settings to the Current Configuration area.

When 1PPort mode is active, the unit uses the Network DLCI values obtained from the Network LMI status response message to automatically configure for each DLCI a corresponding DLCI for Port 1 having the same numeric value as the Network DLCI, and automatically cross connects them. The DLCIs created on the network side are IP Enabled (not standard or multiplexed) DLCIs. In addition, payload management is configured for the network DLCI and assigned the Node IP Address.

Configuration options set by selecting a discovery mode can be manually modified, refined, or deleted at any time using the Configuration menus. No previously discovered and configured DLCIs or cross-connections will be removed unless authorized or Automatic Circuit Removal is enabled (see *Automatically Removing a Circuit* on page 4-11). Additional discovered DLCIs will be configured according to the current Frame Relay Discovery Mode setting. Selecting or changing the setting will not affect IP Addresses or Subnet Masks.

NOTE:

When auto-configuration creates a multiplexed DLCI, but a standard DLCI is needed, change the DLCI to standard from the network DLCI Records screen: *Configuration→Network→DLCI Records*

When a Frame Relay Discovery Mode is changed and saved, the **`Saving will cause Auto-Configuration to update and Restart. Are you sure?`** prompt appears. No is the default for this prompt.

- If Yes (y) is entered, the **`Delete All DLCIs and PVC Connections?`** prompt appears. No is the default for this prompt.
  - If Yes is entered, all multiplexed DLCIs and PVC Connections are deleted, except for Management PVCs with the user data port as the primary destination and the Management PVC that is designated as TS Management Link.
  - If No is entered, previously discovered and auto-configured option settings will not be removed, but configuration updates due to LMI response messages are performed according to the just saved mode setting.
- If No (n) is entered, or if you exit the screen without responding to the prompt, no Auto-Configuration updates are performed and updates due to LMI response messages are performed according to the previously saved setting.

Automatically Removing a Circuit

Using the automatic circuit removal feature, which comes enabled, network DLCIs and PVCs can be automatically removed from the unit's configuration when the network service provider no longer supports them. Automatic deletion is based upon information from a LMI full status response on an active frame relay link.

When this feature is set to:

- **Enable** – The following will be automatically removed from the unit's configuration:
  - Unsupported network DLCIs and PVC connections that include multiplexed network DLCIs.
  - Standard network DLCIs that are Payload Managed or IP Enabled.
  - Unsupported standard network DLCIs that are not configured as the primary destination in a management PVC.
  - Non-management PVCs in which unsupported standard network DLCIs are included.
  - DLCIs not included in three consecutive LMI full status response messages.
  - LMI status responses that indicate a Deleted status for the DLCI.

  All configured options relating to the deleted circuits are also deleted and they revert to their default settings.

  A DLCI will not be deleted if the physical interface or frame relay link is down, or if the DLCI is used for the TS Management Link.
- **Disable** – Unused network DLCIs, PVC connections, and management PVCs must be manually removed.

  If the model has ISDN backup capability, ISDN Link Profiles associated with the deleted records and alternate destinations will be deleted, as well.

Setting Up Dial Backup

When configuring units with ISDN backup capability, the following guidelines apply:

- **Central site** configuration guidelines:
  - Set up the ISDN DBM physical interface.
  - If a BRI DBM, change the Automatic Backup Configuration to Multi_Site_Backup. (A PRI DBM is already configured for multisite backup.)
  - Modify the Link Profile(s) that Automatic Backup Configuration created to add a phone number.
- **Remote site** configuration guidelines:
  - Set up the ISDN DBM physical interface.
  - If a PRI DBM, change the Automatic Backup Configuration to Single_Site_Backup. (A BRI DBM is already configured for single-site backup.)
  - Modify the HQ_Site Link Profile that Automatic Backup Configuration created to add a phone number.
  - Set the criteria by which automatic backup will take place.

Setting Up the DBM Physical Interface

▶ Procedure

1. Configure the DBM interface.

   Main Menu→Configuration→ISDN→Physical

2. Enable the interface, and enter the Service Profile IDs (SPIDs) and local phone numbers.

3. Save the configuration.

See Table 4-9, ISDN BRI DBM Physical Interface Options, or Table 4-10, ISDN PRI DBM Physical Interface Options, for configuration information.

Setting Up Automatic Backup Configuration

The Automatic Backup Configuration feature is used to automatically create alternate DLCI records and PVC connections on the ISDN DBM (backup) interface for current or newly discovered PVC Connections and Management PVCs.

This feature is already set up, with Single_Site_Backup as the default for units with a BRI DBM and Multi_Site_Backup for units with a PRI DBM. If the unit at the central site has a BRI DBM, change the Automatic Backup Configuration to Multi_Site_Backup, if necessary.

Main Menu→Auto-Configuration→Automatic Backup Configuration

If you select . . .	Then . . .
Single_Site_Backup *(default for a BRI DBM)* *(Used at remote sites since only one ISDN link to the central-site is needed.)*	Alternate destinations are automatically configured using a single ISDN Link Profile to backup all network PVC Connections and Management PVCs over the primary destination ISDN link. Initially, PVCs with alternate destinations are configured on the first ISDN Link Profile using the same DLCI number as the network DLCI being backed up. However, primary destination PVCs on the ISDN DBM interface are automatically updated to use a different DLCI number for the alternate destination DLCI, derived from the first SLV message received on the each network DLCI.
Multi_Site_Backup *(default for a PRI DBM)* *(Used at central sites since multiple ISDN links are needed, one for each remote-site.)*	Alternate destinations are automatically configured using a separate ISDN Link Profile to backup each network PVC Connection and Management PVC over the ISDN interface. Initially, all DLCIs are configured on the ISDN links using the same DLCI number as the network DLCI being backed up. However, primary destination PVCs on the ISDN DBM interface are automatically updated to use a different DLCI number for the alternate destination DLCI, derived from the first SLV message received on the each network DLCI. Automatically created alternate destination Link Profiles appear as Bkup*nnnn*, *nnnn* being the DLCI number (e.g., Bkup200 would be configured for network DLCI 200).
Disabled	No automatic configuration takes place on the DBM interface and no alternate destinations are created for PVCs.

NOTE:

Changes must be saved to take effect.

See *Setting Up Auto-Configuration* on page 4-8, to see a screen example.

When the Automatic Backup Configuration setting is changed, the following prompts appear. No is the default for these prompts.

When the . . .	The following prompt appears . . .	If you select . . .
■ Automatic Backup Configuration setting was changed, and ■ Save was selected	**Saving will cause Auto-Configuration to update and Restart. Are you sure?**	■ No – No Auto-Configuration updates are performed and updates due to LMI response messages are performed according to the previously saved setting. ■ Yes – The **Delete All DLCIs and PVC Connections?** prompt appears.
■ Response to the **Delete All DLCIs and PVC Connections?** prompt was No, and ■ Automatic Backup Configuration was disabled	**Delete All Alternate Destinations from PVC Connections?**	■ No – No previously configured DLCIs or PVC connections are removed or changed, and newly discovered DLCIs will be configured according to the new discovery mode and automatic backup setting. ■ Yes – All multiplexed DLCIs, ISDN Link Profiles (except for the first one), and PVC connections are deleted, except for management PVCs with the user data port as the primary destination and management PVCs designated as the TS Management Link. If an alternate destination has been configured on a retained Management PVC, the alternate destination will be deleted but the primary destination will be retained.
■ Response to the **Delete All DLCIs and PVC Connections?** prompt was No, and ■ Automatic Backup Configuration was set to Single_Site_Backup or Multi_Site_Backup	**Add Alternate Destinations to Current PVC Connections?**	■ Yes – DLCI records are configured on the ISDN link(s) and Alternate Destination information is added to current PVC connections and management PVCs. ■ No – No previously configured PVC connections are changed, and newly discovered DLCIs will be configured according to the new discovery mode and automatic backup setting.

When the . . .	The following prompt appears . . .	If you select . . .
■ Response to the **Remove Alternate Destinations from PVCs and delete unused DLCI Records?** prompt was Yes, and ■ Automatic Backup Configuration was disabled	—	■ No – No previously configured DLCIs, ISDN Link Profiles, or PVC Connections are removed or changed, but updates due to LMI responses will be performed using the new setting. ■ Yes – All Alternate Destination information will be removed from PVC Connections and Management PVCs, and all DLCIs and ISDN Link Profiles (except for the first one) used exclusively as Alternate Destinations are deleted.
■ Response to the **Remove Alternate Destinations from PVCs and delete unused DLCI Records?** prompt was Yes, and ■ Automatic Backup Configuration was set to Single_Site_Backup or Multi_Site_Backup	**Add Alternate Destinations to Current PVC Connections?**	■ No – No previously configured PVC Connections are removed or changed, but updates due to LMI responses will be performed using the new setting. ■ Yes – Alternate Destination information is configured for current DLCIs, ISDN Link Profiles, PVC Connections and Management PVCs on the ISDN DBM interface, except for the Management PVC designated as the TS Access Management Link.

NOTE:

When DLCIs, PVC connections, and management PVCs for the first ISDN Link Profile have been configured manually, it is recommended that specific discovered DLCIs, PVC connections, and management PVCs be deleted manually via the Configuration menus. Otherwise, the manual configurations will be deleted along with the automatically configured ones.

To specify when automatic backup is allowed or can occur, see *Configuring the Criteria for Automatic Backup* on page 4-104.

Modifying ISDN Link Profiles

Once an ISDN Link Profile is configured using the Automatic Backup Configuration feature, phone numbers and Calling IDs need to be entered. FrameSaver units with ISDN backup capability can originate or answer calls, as needed, so both phone numbers and Calling IDs are needed.

▶ Procedure

1. Select Link Profiles, then Modify.

   Main Menu→Configuration→ISDN→Link Profiles

2. Add a name and phone number to the ISDN Link Profile(s) created by Automatic Backup Configuration.

   — Name for the destination entered (e.g., Tampa). The default setting is HQ_Site for the first ISDN Link Profile.

   — Phone numbers entered:

For Originating a Backup Call	**For Answering a Backup Call**
Outbound and Alternate Outbound phone numbers Valid characters can include: ■ Numbers (0–9) ■ Special characters * and # ■ Spaces ■ Parentheses ( )	Inbound Calling ID1 and ID2 These are the phone numbers of units from which calls will be accepted. Valid characters can include: ■ Numbers (0–9)

   NOTES:

   Remember to include local dial-out numbers (i.e., 9, then the number).

   For every originating (outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa.

   — Maximum Link Rate (Kbps) set to the appropriate speed, if necessary.

   — Caller Identification Method set to Proprietary if call validation is not required. The setting must be the same at both ends of the circuit.

   — An Alternate Outbound Phone Number should a call using the primary Outbound Phone Number be unsuccessful, if desired.

3. Save the configuration.

See Table 4-11, ISDN Link Profile Options, for configuration information.

Restricting Automatic Backup and Configuring Backup Timers

You can specify when auto backup is allowed to occur. If backup is restricted and a backup is active when the allowed time for backups is over, then the backup is terminated and the data is returned to the primary data path regardless of the primary path's condition.

You can restrict auto backup to occur only:

- On certain days of the week
- At certain times of the day

The following additional features can be configured:

- Delays can be configured to control how long the unit will wait before initiating backup when a DLCI is declared down, and how long it will wait to restore service once the DLCI is declared operational again.
- A threshold can be set to determine how many times a primary destination DLCI can transition between Active and Inactive before the unit initiates backup.

▶ Procedure

To set the criteria and backup timers for automatic backup:

1. Enable Auto Backup.

   Main Menu→Configuration→Auto-Backup Criteria

   When a failure occurs, the unit automatically enables the Alternate Link and traffic is rerouted over the backup (alternate) interface.

2. Specify the amount of delay after a DLCI is declared down before backup is initiated (DLCI Down Backup Activation Delay).
3. Set the threshold for transitions of the DLCI's status before backup is initiated (DLCI Down Backup Activation Transmission Threshold).
4. Specify the amount of delay after a DLCI is declared operation before backup is ended (Backup Restoration Delay).
5. Specify When Auto Backup Allowed – Always or Restrict. If Restrict is selected, specify the days and hours of the week during which automatic backup can take place.
6. Save the configuration.

See Table 4-26, Auto Backup Criteria Options, for configuration information.

Configuring the DBM Interface to Send SNMP Traps

The ISDN DBM interface can be specified as an interface that monitors and generates SNMP traps:

Main Menu→Configuration→Management and Communications→ SNMP Traps

The configuration options for doing this include:

- Link Trap Interfaces
- DLCI Traps on Interfaces
- ISDN Dial Control Traps

When DBM is selected, trap messages are generated for linkUp and linkDown events on DLCIs and frame relay links for the originating DBM interface only. For peer-to-peer backup, backing up to a neighboring node like a regional node, dial control traps can be sent to trap manager(s).

See Table 4-22, SNMP Traps and Trap Dial-Out Options, for configuration information.

Assigning DLCIs to a Backup Group

DLCIs can be assigned to a Backup Group to reduce backup charges when redundant PVCs have been configured. This feature prevents backup as long as any DLCI in the group is operational.

- Backup is not initiated as long as one DLCI in the group is operational.
- Backup is terminated as soon as one DLCI in the group becomes operational.

See Table 4-14, DLCI Record Options, for configuration information.

PVC Backup Over the Network Interface

Generally, backup can be performed on the network interface’s frame relay link using a backup PVC, as well on an ISDN link; the unit does not have to have the ISDN DBM feature.

In this case, create a DLCI Record on the network interface that will be used for backup, then modify the PVC Connections or Management PVCs to add the alternate destination.

Setting Up Back-to-Back Operation

Using this special feature, you can set up two FrameSaver units that are connected back-to-back without frame relay switches between them, as in a test bench setup using a crossover cable.

Changing Operating Mode

When setting up back-to-back operation:

- One unit must be configured for Standard operation, which is the setting for normal operation.
- The other unit must be configured for Back-to-Back operation so it presents the network side of the UNI (user-network interface).

Only one of the units will have its operating mode changed.

▶ Procedure

To set up back-to-back operation:

1. On the unit to be configured for Back-to-Back operation, manually configure DLCIs; DLCIs should be configured before connecting the two units.
2. Access the Change Operating Mode screen.

   Main Menu→Control→Change Operating Mode

3. Select Back-to-Back Operation, and respond Yes to the **`Are you sure?`** prompt.
4. Save the change.

▶ Procedure

To return the unit to normal operation:

1. Return to the Change Operating Mode screen and switch back to Standard Operation.
2. Respond Yes to the prompt and save the change. The units can be reconnected to a standard frame relay network.

Configuration Option Tables

Configuration option descriptions contained in this chapter are in menu order, even though this may not be the order in which you access each when configuring the unit.

The following configuration option tables are included:

- Table 4-1, System Frame Relay and LMI Options
- Table 4-2, Class of Service Definitions
- Table 4-3, Code Point Definitions
- Table 4-4, Service Level Verification Options
- Table 4-5, General System Options
- Table 4-6, Network Physical Interface Options
- Table 4-7, Data Port Physical Interface Options
- Table 4-8, DSX-1 Physical Interface Options
- Table 4-9, ISDN BRI DBM Physical Interface Options
- Table 4-10, ISDN PRI DBM Physical Interface Options
- Table 4-11, ISDN Link Profile Options
- Table 4-12, Signaling and Trunk Conditioning Values (when Assigning DSX-1-to-Network Time Slots/Cross Connections)
- Table 4-13, Interface Frame Relay Options
- Table 4-14, DLCI Record Options
- Table 4-15, PVC Connection Options
- Table 4-16, IP Path List
- Table 4-17, Node IP Options
- Table 4-18, Management PVC Options
- Table 4-19, General SNMP Management Options
- Table 4-20, Telnet and FTP Session Options
- Table 4-21, SNMP NMS Security Options
- Table 4-22, SNMP Traps and Trap Dial-Out Options
- Table 4-23, Ethernet Management Options
- Table 4-24, Communication Port Options
- Table 4-25, Modem Port Options
- Table 4-26, Auto Backup Criteria Options

Configuring the Overall System

The System menu options are explained in the following sections:

- *Configuring Frame Relay and LMI for the System (CSU/DSUs)*
- *Configuring Service Level Verification Options*
- *Configuring General System Options*

Configuring Frame Relay and LMI for the System (CSU/DSUs)

Select Frame Relay and LMI from the System menu to display or change the Frame Relay and LMI options for the entire system (see Table 4-1, System Frame Relay and LMI Options).

Main Menu→Configuration→System →Frame Relay and LMI

See *Configuring Frame Relay for an Interface* on page 4-61 to set an interface's frame relay options.

Table 4-1. System Frame Relay and LMI Options (1 of 4)

LMI Behavior
Possible Settings: **Independent,** Net1-FR1_Follows_Port-1, Net1-FR1_Follows_Port-2, Net1-FR1_Follows_Rtr-S0, Port-1_Follows_Net1-FR1, Port-2_Follows_Net1-FR1, Rtr-S0_Follows_Net1-FR1, All_Ports_Follow_Net1-FR1, Port-1_Codependent_with_Net1-FR1, Port-2_Codependent_with_Net1-FR1, Rtr-S0_Codependent_with_Net1-FR1, Default Setting: **Independent**
Configures the device to allow the state of the LMI to be passed from one interface to another, determining how the unit will handle a change in the LMI state. Sometimes referred to as LMI pass-through. *Display Conditions* – Port-*n* options are available on CSU/DSUs and Rtr-S0 options are available on the FrameSaver SLV 9126-II Router. NOTE: LMI Behavior cannot be changed while Auto Backup is enabled. A warning message appears at the bottom of the screen if auto backup is enabled. First, disable Auto Backup, and then change LMI Behavior. **Independent** – Handles the LMI state of each interface separately so that the LMI state of one interface has no effect on the LMI state of another interface. Provides LMI Spoofing. This is the recommended setting when backup is configured, and for Network Service Providers (NSPs).

Table 4-1. System Frame Relay and LMI Options (2 of 4)

LMI Behavior *(continued)*
Net1-FR1_Follows_Port-1 – Brings LMI down on the network interface when LMI on Port-1 goes down, disabling the network interface and deasserting its control leads. When LMI on Port-1 comes back up, the network interface is reenabled. The LMI state on the network interface has no effect on the LMI state on Port-1. That is, the network interface's LMI follows Port-1's LMI. Used at central sites, this setting is useful when the remote site router on the other end of the PVC connection can initiate recovery via a redundant central site when there is a catastrophic central site LAN or router failure. Not recommended for NSPs.
Net1-FR1_Follows_Port-2 – Reacts like the Net1-FR1_Follows_Port-1 selection, but for Port-2 instead.
Rtr-S0_Follows_Port-1 – Brings LMI down on the network interface when LMI on Rtr-S0 goes down, disabling the network interface and deasserting its control leads. When LMI on Rtr-S0 comes back up, the network interface is reenabled. The LMI state on the network interface has no effect on the LMI state on Rtr-S0. That is, the network interface's LMI follows Rtr-S0's LMI.
Port-1_Follows_Net1-FR1 – Brings LMI down on Port-1 when LMI on the network interface goes down, disabling Port 1 and deasserting its control leads. When LMI on the network interface comes back up, Port-1 is reenabled and its control leads are reasserted. The LMI state on Port-1 has no effect on the LMI state on the network interface. That is, Port-1's LMI follows the network interface's LMI. This setting is useful if the router connected to Port-1 is used to initiate recovery when network failures are detected.
Port-2_Follows_Net1-FR1 – Reacts like the Port-1_Follows_Net1-FR1 selection, but for Port-2 instead.
Rtr-S0_Follows_Net1-FR1 – Brings LMI down on Rtr-S0 when LMI on the network interface goes down, disabling Rtr-S0. When LMI on the network interface comes back up, Rtr-S0 is reenabled. The LMI state on Rtr-S0 has no effect on the LMI state on the network interface. That is, Rtr-S0's LMI follows the network interface's LMI.
All_Ports_Follow_Net1-FR1 – Brings LMI down on all user data ports when LMI on the network interface goes down, disabling all ports and deasserting their control leads. Allows LMI to come back up and reenables the ports when LMI comes up on the network. That is, LMI on each port follows the network interface's LMI. The state of LMI on the port will not affect the state of LMI on the network interface.
Port-1_Codependent_with_Net1-FR1 – Brings LMI down on the network interface when LMI on Port-1 goes down (or LMI down on Port-1 when LMI on the network interface goes down), and allows LMI to come back up when LMI comes back on the other interface. That is, the LMI state for one interface is dependent on the other. Use this setting when backup is through the router instead of the unit. It is *not* recommended since it makes fault isolation more difficult.
Port-2_Codependent_with_Net1-FR1 – Reacts like the Port-1_Codependent_with_Net1-FR1 selection, but for Port-2 instead. The state of LMI on the network interface will not affect the state of LMI on Port-1.
Rtr-S0_Codependent_with_Net1-FR1 – Brings LMI down on the network interface when LMI on Rtr-S0 goes down (or LMI down on Rtr-S0 when LMI on the network interface goes down), and allows LMI to come back up when LMI comes back on the other interface. That is, the LMI state for one interface is dependent on the other.

Table 4-1. System Frame Relay and LMI Options (3 of 4)

LMI Error Event (N2)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **3**
Configures the LMI-defined N2 parameter, which sets the number of errors that can occur on the LMI link before an error is reported. Applies to both the user and network sides of a UNI. **1 – 10** – Specifies the maximum number of errors.
LMI Clearing Event (N3)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **1**
Configures the LMI-defined N3 parameter, which sets the number of error-free messages that must be received before clearing an error event. Applies to both the user and network sides of a UNI. **1 – 10** – Specifies how many error-free messages it will take to clear the error event.
LMI Status Enquiry (N1)
Possible Settings: **1, 2, 3, 4, . . . 255** Default Setting: **6**
Configures the LMI-defined N1 parameter, which sets the number of status enquiry polling cycles that the user side of the LMI initiates before a full status enquiry is initiated. Applies to the user side of a UNI only. **1 – 255** – Specifies the number of status enquiry polling cycles that can be initiated before a full status enquiry is initiated.
LMI Heartbeat (T1)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **10**
Configures the LMI-defined T1 parameter, which sets the number of seconds between the initiation of status enquiry messages on the user side of the LMI. Applies to the user side of a UNI only. **5 – 30** – Specifies the number of seconds between the initiation of status enquiry messages in increments of 5.
LMI Inbound Heartbeat (T2)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **15**
Configures the LMI-defined T2 parameter, which sets the number of seconds between the receipt of status enquiry messages on the network side of the LMI. Applies to the network side of a UNI only. **5 – 30** – Specifies the number of seconds between the receipt of status enquiry messages in increments of 5.

Table 4-1. System Frame Relay and LMI Options (4 of 4)

LMI N4 Measurement Period (T3)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **20**
Configures the LMI-defined T3 parameter, which is the time interval (in seconds) that the network side of the LMI uses to measure the maximum number of status enquiry messages that have been received (N4) from the user side. **5 – 30** – Specifies the interval of time in increments of 5.

Configuring Class of Service Definitions

Select Class of Service Definitions from the System menu to display or change the Class of Service definitions to be used with latency, availability, and throughput measurements of IP traffic on IP Enabled circuits.

Main Menu→Configuration→System →Class of Service Definitions

The Class of Service Definitions screen appears.

▶ Procedure

To create a new Class of Service definition:

1. To manually assign definition names and code points, proceed to Step 4
2. To automatically create Class of Service names and associate them with code points according to RFCs 2474, 2497, and 2498, select RfcCodePoints. The following settings are established:

Field	Setting After RfcCodePoints Selected
Class of Service Name	1 – NewCtrl 2 – Expd Fwd 3 – AFClass4 4 – AFClass3 5 – AFClass2 6 – AFClass1 7 – Default
Measure Latency & Availability	1 – N 2 – Y 3 – Y 4 – Y 5 – Y 6 – Y 7 – Y
Code Points	1 (NetwCtrl) – 110000, 111000 2 (Expd Fwd) – 101110 3 (AFClass4) – 100010, 100100, 100110 4 (AFClass3) – 011010, 011100, 011110 5 (AFClass2) – 010010, 010100, 010110 6 (AFClass1) – 001010, 001100, 001110 7 (Default) – 000000

3. If these settings are satisfactory, proceed to Step 10.
4. Type a name of up to 8 characters into one of the Name fields next to IDs 1–6.
5. To unassign all code points by inserting blank names, select ClrAllCodePoints. To assign all Code Points to a Class of Service name of Default, select DefaultCodePoints.
6. Select PgDn or PgUp. The Code Point Assignment screen appears.
7. For any Code Point you want to assign to the name, type the name you selected in Step 4 into the Name field to the right of the Code Point.

8. Select Save, then select PgDn or PgUp. The Class of Service Definitions page reappears. In the Code Points Assigned column next to your selected name there is now a Y for Yes.
9. If latency and availability should be measured for the selected name, change the N in the Measure Latency & Availability column to Y.
10. Select Save.

To configure these options, Service Type on the Easy Install screen must be set to Frame Relay.

Table 4-2. Class of Service Definitions

Class of Svc Name
Possible Settings: ***ASCII Text Entry*** Default Setting: *For IDs 2–7:* **blank** *For ID 1:* **Default**
Specifies a name to identify a Class of Service definition. ***ASCII Text Entry*** – Enter a unique name for the definition (maximum length 8 characters).
Measure Latency & Availability
Possible Settings: **N, Y** Default Setting: *For IDs 2–7:* **N** *For ID 1:* **Y**
Determines whether latency and availability are measured for this Class of Service ID. *Display Conditions* – This option is set to N and is read-only until the class of service is defined and code points are assigned to it. **N** – Latency and availability are not measured for this Class of Service ID. **Y** – Latency and availability are measured for this Class of Service ID.
Code Points Assigned
Possible Settings: **Y, N** Default Setting: *For IDs 2–7:* **N** *For ID 1:* **Y**
This read-only field shows whether a Code Point has been assigned to this Class of Service ID on the Code Point Definitions screen. **N** – No Code Point is assigned to this ID. **Y** – At least one Code Point is assigned to this ID.

Code Point Definitions

Select Class of Service Definitions from the System menu, then PgDn or PgUp, to display or change the Code Point definitions for a Class of Service ID. See *Configuring Class of Service Definitions* on page 4-25 for instructions.

Table 4-3. Code Point Definitions

Code Pnt
Possible Settings: **000000–111111** Default Setting: None.
This read-only field shows the possible Code Points. Code Points are described in RFC 2474.
ID
Possible Settings: **1–7** Default Setting: **1**
This read-only field shows the ID associated with the Name field. If you change a name in a Name field on this screen and select Save, the ID changes to match the name.
Name
Possible Settings: ***ASCII Text*** Default Setting: **Default**
The Name field specifies the Class of Service to which you want to assign the Code Point. ***ASCII Text*** – Specifies one of the Class of Service Names entered on the Class of Service Definitions screen.

Configuring Service Level Verification Options

SLV options are selected from the System menu (see Table 4-4, Service Level Verification Options).

Main Menu→Configuration→System→Service Level Verification

Table 4-4. Service Level Verification Options (1 of 3)

SLV Sample Interval (secs)
Possible Settings: **10 – 3600** Default Setting: **60**
Sets the inband communications interval between FrameSaver SLV devices. Inband communications are used to pass frames that calculate latency, as well as transmission success and other SLV information. **10 – 3600** – Sets the SLV Sample Interval (secs) in seconds.
SLV Synchronization Role
Available Settings: **Tributary, Controller, None** Default Setting: **Tributary**
Determines the role the unit plays in maintaining synchronization of user history data collection and storage between FrameSaver SLV and/or FLEX devices. **Tributary** – Uses network timing received from incoming SLV communications and provides network-based synchronization information to other devices in the network. **Controller** – Uses its own internal time-of-day clock and provides synchronization information to other devices in the network based upon its own clock. NOTE: Only one device in the network should be configured as the SLV synchronization controller. **None** – Incoming timing information is ignored and no timing information is sent out. This setting should only be used when network synchronization is not desirable, or when a single unit connects multiple networks or network segments.
SLV Type
Available Settings: **Standard, COS 1–COS 7** Default Setting: *If SLV Feature is enabled:* **Standard** *If SLV Feature is disabled:* **COS 1**
Determines the type of SLV measurements to which these other SLV options apply: ■ SLV Timeout Error Event Threshold ■ SLV Timeout Clearing Event Threshold ■ SLV Round Trip Latency Error Threshold ■ SLV Latency Clearing Event Threshold ■ SLV Packet Size **Standard** – The options selected apply to standard FrameSaver SLV measurements, utlizing an EDLCI for FrameSaver-to-FrameSaver communication. This option is not available if the SLV Feature is disabed. **COS 1–COS 7** – The options selected apply to this Class of Service. Different settings may be saved for each Class of Service.

Table 4-4. Service Level Verification Options (2 of 3)

SLV Delivery Ratio
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether communication of Frame and Data Delivery Ratios (FDR/DDR) between FrameSaver SLV devices is enabled. To use this capability, both ends of all PVCs must be FrameSaver SLV devices. If some of the units are FrameSaver 9124s or 9624s, they must be running software version 1.2 or higher. *Display Conditions* – This option appears only if SLV Type is Standard. **Enable** – An extra byte for FDR/DDR statistics collection is included with each frame, which is used at the receiving end to determine the amount of data dropped by the network. **Disable** – Extra byte is not included.
DLCI Down on SLV Timeout
Available Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether missed SLV packets will be monitored along with the LMI status to determine the status of PVC connections to remote FrameSaver units. NOTE: This option does not apply to multiplexed DLCIs connected to a far-end unit with hardware bypass capability. *Display Conditions* – This option appears only if SLV Type is Standard. **Enable** – After the configured threshold for missed SLV packets has been exceeded, causing the DLCI's status to turn Inactive, an alarm and SNMP trap are generated, and a Health and Status message created. **Disable** – Missed SLV packets are monitored, but the DLCI is not declared down.
SLV Timeout Error Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **3**
Specifies the number of consecutive missed SLV communications that must be detected before a DLCI Inactive status is declared. **1–20** – Sets the limit for these error events.
SLV Timeout Clearing Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **1**
Specifies the number of consecutive SLV messages that must be received before the DLCI Inactive status is cleared. **1 – 20** – Sets the limit for the clearing event.

Table 4-4. Service Level Verification Options (3 of 3)

SLV Round Trip Latency Error Threshold (ms)
Available Settings: **50, 51, 52, . . . 10000** Default Setting: **10000**
Specifies the number of milliseconds that must be exceeded before an SLV Latency Threshold alarm event is declared and backup, if configured, is initiated for a DLCI. If SLV Type is Standard, the latency applies to a multiplexed DLCI. If SLV Type is a Class of Service (COS 1 – COS 7), the latency applies to the COS on an IP Enabled path. **50–10000** – Sets the limit for these error events.
SLV Latency Clearing Event Threshold
Available Settings: **1, 2, 3, 4 . . . 20** Default Setting: **2**
Specifies the number of consecutive SLV latency measurements below the error threshold that must be received before the error status is cleared. **1 – 20** – Sets the limit for the clearing event.
SLV Packet Size (bytes)
Available Settings: **64 – 2048** Default Setting: **64**
Sets the size of packets, in bytes, that will be used for SLV communications. SLV packets are used to track latency and other SLV-related variables. When the packet size is changed, a new round trip and average latency calculation must be performed, so these measurements will not appear on the SLV Performance Statistics screen until a new sampling interval has occurred. **64 – 2048** – Sets the packet size for SLV communications.

Configuring General System Options

Select General from the System menu to configure the general system configuration options (see Table 4-5, General System Options).

Main Menu→Configuration→System→General

Table 4-5. General System Options (1 of 3)

Test Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether or not loopback and pattern tests have a duration after which they are terminated automatically. **Enable** – All Loopback and Pattern tests have a timeout. This setting is recommended when the FrameSaver unit is managed remotely through an in-band data stream. If the FrameSaver unit is accidently commanded to execute a disruptive test on the interface providing the management access, control can be regained after the timeout expires, terminating the test. **Disable** – Loopback and pattern tests must be manually terminated.
Test Duration (min)
Possible Settings: **1 – 120** Default Setting: **10**
Specifies the maximum duration of the tests. *Display Conditions* – This option only appears when Test Timeout is set to Enable. **1 – 120** – Sets the Test Timeout period in minutes (inclusive).
Primary Clock Source
Possible Settings: **Net1, DSX, Internal, DBM** Default Setting: **Net1**
Allows you to select the primary clock source for the unit. The source selected provides all of the timing within the FrameSaver unit and the clocks for all of the external interfaces. Failure of the clock specified by this configuration option results in automatic fallback to the Secondary Clock Source configuration option setting. NOTE: For the Primary and Secondary Clock Source options, only Internal can be selected for both options. All other selections must have different settings (e.g., if Primary Clock Source is set to Net1, Secondary Clock Source cannot be set to Net1). **Net1** – The primary clock is derived from the Network1 T1 interface. **DSX** – The primary clock for the unit is derived from the DSX-1 interface. This setting only appears if the DSX-1 interface is enabled (see *Configuring the DSX-1 Interface* on page 4-43). **Internal** – The primary clock is the internal clock. **DBM** – The primary clock is derived from the DBM. This selection only appears if the DBM is installed and enabled.

Table 4-5. General System Options (2 of 3)

Secondary Clock Source
Possible Settings: **Net1, DSX, Internal, DBM** Default Setting: **Internal**
Provides a secondary clock source when the primary clock source fails. The source selected for this configuration option provides all of the timing within the unit and the clocks for all of the external interfaces. The clock source will switch back to primary when the primary clock source returns and is stable for 10 seconds. If the secondary clock source fails, the clock source will switch to internal. The clock source will switch back to primary when the primary clock source returns and is stable for 10 seconds. NOTE: For the Primary and Secondary Clock Source options, only Internal can be selected for both options. All other selections must have different settings (e.g., if Primary Clock Source is set to Net1, Secondary Clock Source cannot be set to Net1). **Net1** – The secondary clock is derived from the Network1 T1 interface. **DSX** – The secondary clock for the unit is derived from the DSX-1 interface. This setting only appears if the DSX-1 interface is enabled. **Internal** – The secondary clock is the internal clock. **DBM** – The secondary clock is derived from the DBM. This selection only appears if the DBM is installed and enabled.

Table 4-5. General System Options (3 of 3)

System Alarm Relay
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether an alarm condition for the unit will activate the system alarm relay. The alarm relay is deactivated when the condition causing the alarm is corrected. If more than one alarm condition is present, the alarm relay remains active until all alarm conditions are cleared. You can also deactivate an alarm via the System Alarm Relay Cut-Off selection from the Control menu; however, the alarm itself is not cleared. When another alarm condition is detected, the alarm is reactivated again, requiring another manual deactivation of the alarm relay. *Display Conditions* – This option only appears for a FrameSaver SLV 9128-II installed in the 9000 Series Access Carrier. Alarm conditions are: ■ Alarm Indication Signal (AIS) received at the Network, DSX-1, or PRI interface ■ Continuous Loss of Signal (LOS) condition at the Network, DSX-1, or PRI interface ■ CTS Down ■ DBM Download Required ■ DBM BRI Card Failed ■ Device Fail ■ DLCI Down ■ DTR Down ■ Ethernet Link Down ■ Excessive Error Rate (EER) detected at the Network or PRI interface ■ Internal Modem Failed ■ ISDN Network Failure ■ LMI Down ■ Network Communication Link Down ■ Out of Frame (OOF) at Network, DSX-1, or PRI ■ Primary or Secondary Clock Failure ■ Power Supply/Fan Failure ■ RTS Down ■ Self-Test Failure ■ SLV Latency Exceeded ■ SLV Timeout ■ Suboptimal (Maximum) Link Rate Cannot be Achieved ■ Two Level-1 Users Accessing Device ■ Yellow Alarm Signal on the Network, DSX-1, or PRI interface **Enable** – Activates alarm conditions on the system alarm relay when an alarm condition occurs. **Disable** – Does not activate the system alarm relay when an alarm condition occurs.

Configuring Physical Interfaces

Characteristics for physical interfaces are explained in the following sections:

- *Configuring the Network Interface*
- *Configuring a User Data Port (CSU/DSUs)*
- *Configuring the DSX-1 Interface*
- *Configuring the ISDN DBM Interface*

Configuring the Network Interface

When configuring the physical characteristics for the network interface, select Physical from the Network menu (see Table 4-6, Network Physical Interface Options).

Main Menu→Configuration→Network→Physical

Table 4-6. Network Physical Interface Options (1 of 4)

Line Framing Format
Possible Settings: **D4, ESF** Default Setting: **ESF**
Specifies the framing format for transmitted and received signals on the T1 network interface. **D4** – Uses D4 framing format. NOTE: This setting is not recommended by network carriers. False yellow alarms may occur after traffic has been running and the channel returns to idle, or when there is light traffic when other settings are selected. ESF format does not create this problem. **ESF** – Uses Extended Superframe framing format.
Line Coding Format
Possible Settings: **AMI, B8ZS** Default Setting: **B8ZS**
Specifies the line coding format for the network interface. **AMI** – Uses Alternate Mark Inversion (AMI) line coding format. **B8ZS** – Uses Bipolar 8 Zero Substitution (B8ZS) line coding format.

Table 4-6. Network Physical Interface Options (2 of 4)

Line Build Out (LBO)
Possible Settings: **0.0, –7.5, –15, –22.5** Default Setting: **0.0**
Specifies the line build out for the signal transmitted to the network. **0.0, –7.5, –15, –22.5** – Specifies line build out in dB.
Bit Stuffing
Possible Settings: **62411, Disable** Default Setting: **62411**
Determines the type of bit insertion to provide ones density requirements for data transmitted to the network. *Display Conditions* – This option does not appear when Line Coding Format is set to B8ZS. **62411** – Inserts a one in the data after 15 consecutive zeros are received or the density of ones falls below 12.5%. This setting complies with AT&T TR 62411, but is not recommended for frame relay data because it inserts errors in the data traffic. **Disable** – Disables bit stuffing. Ones density is not enforced on data sent to the network.
Transmit Timing
Possible Settings: **System, Interface** Default Setting: **System**
Allows transmit timing to be selected from either the system master clock source or from the currently selected interface. **System** – Transmit timing is derived from the current system clock source (see Table 4-5, General System Options). **Interface** – Transmit timing is derived from this interface. NOTE: When Interface is configured, the clock must be synchronized to the system clock source.
Network Initiated LLB
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Allows the initiation and termination of the line loopback (LLB) to be controlled by the receipt of LLB-Actuate and LLB-Release commands from the network. **Enable** – LLB is controlled by LLB-Actuate and LLB-Release commands. Receiving a LLB-Actuate command causes the FrameSaver unit to enter a line loopback (provided an LLB can be performed in the FrameSaver unit's current state). Receiving an LLB-Release command terminates the LLB. **Disable** – The FrameSaver unit ignores the LLB-Actuate and LLB-Release commands. NOTE: When disabled, the system is not in compliance with ANSI T1.403 or AT&T TR 62411.

Table 4-6. Network Physical Interface Options (3 of 4)

Network Initiated PLB
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Allows the initiation and termination of the payload loopback (PLB) to be controlled by the receipt of PLB-Actuate and PLB-Release commands from the network. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **Enable** – PLB is controlled by PLB-Actuate and PLB-Release commands. Receiving a PLB-Actuate command causes the system to enter a payload loopback (provided a PLB can be performed in the unit's current state). Receiving a PLB-Release command terminates the PLB. **Disable** – The FrameSaver unit ignores the PLB-Actuate and PLB-Release commands. NOTE: When disabled, the unit is not in compliance with ANSI T1.403 or AT&T TR 54016.
Network Initiated DCLB
Possible Settings: **Disable, V.54_&_ANSI** Default Setting: **V.54_&_ANSI**
Allows the initiation and termination of the Data Channel Loopback (DCLB V.54 Loop 2) to be controlled by the receipt of a DCLB-actuate or DCLB-release sequence (either V.54 or FT1-ANSI compliant) from the network on the DS0s used for the network frame relay link. When enabled and a DCLB-activate sequence is received, the unit initiates a DCLB on the network interface. When a DCLB-release sequence is received, the DCLB is stopped. **Disable** – DCLB-actuate and DCLB-release sequences are ignored. **V.54_&_ANSI** – DCLB-actuate and DCLB-release sequences that comply with either V.54 or ANSI T1.403, Annex B standard will be recognized and will control initiation and termination of a DCLB for the network frame relay link. The actuate and release sequences do not need to match (for example, a DCLB started with a V.54 actuate sequence can be stopped with an FT1 release sequence).
ANSI Performance Report Messages
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether ANSI T1.403 compliance performance report messages (PRMs) are generated and sent to the network over the ESF facility data link every second. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **Enable** – Generates and sends PRMs. **Disable** – Does not generate and send PRMs.

Table 4-6. Network Physical Interface Options (4 of 4)

Excessive Error Rate Threshold
Possible Settings: **10E-4, 10E-5, 10E-6, 10E-7, 10E-8, 10E-9** Default Setting: **10E-4**
Sets the error rate threshold that determines when an EER condition is declared. The excessive error rate is determined by the ratio of the number of CRC6 errors to the total number of bits received over a set period of time. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **10E-4** – Declares an EER if more than 1,535 CRC6 errors are detected in a 10 second period. Clears when fewer than 1,536 CRC6 errors are detected within the same time period. **10E-5** – Declares an EER if more than 921 CRC6 errors are detected in a 60 second period or a 10^{-4} condition occurs. Clears when fewer than 922 CRC6 errors are detected within the same time period. **10E-6** – Declares an EER if more than 92 CRC6 errors are detected in a 60 second period or a 10^{-5} or 10^{-4} condition occurs. Clears when fewer than 93 CRC6 errors are detected within the same time period. **10E-7** – Declares an EER if more than 9 CRC6 errors are detected in a 60 second period or a 10^{-6}, or 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 10 CRC6 errors are detected within the same time period. **10E-8** – Declares an EER if more than 41 CRC6 errors are detected in three 15 minute intervals or a 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} condition occurs. Clears when fewer than 42 CRC6 errors are detected within the same time period. **10E-9** – Declares an EER if more than 4 CRC6 errors are detected in three 15 minute intervals or a 10^{-8}, 10^{-7}, 10^{-6}, 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 5 CRC6 errors are detected within the same time period.
Circuit Identifier
Possible Settings: ***ASCII Text Entry*, Clear** Default Setting: **blank**
Identifies the transmission vendor's circuit information to facilitate troubleshooting. ***ASCII Text Entry*** – Edit or display circuit identifier information (maximum 255 characters). **Clear** – Removes the circuit identifier information.

Configuring a User Data Port (CSU/DSUs)

Select Physical from the Data Ports menu to display or change the physical characteristics of the data port connected to the DTE (see Table 4-7, Data Port Physical Interface Options).

Main Menu→Configuration→Data Ports→Physical

Table 4-7. Data Port Physical Interface Options (1 of 5)

Port Status
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the data port is being used and can be configured. **Enable** – The port is active, and can be used to transmit and receive data. **Disable** – The port is not active. When the port is disabled, the following will occur: ■ No alarms or traps configured for the port will be generated. ■ LED for the port will be held in an Off state. **No** – The operation is cancelled. (Pressing either the Esc or Ctrl-a key also acts as a No.) **Yes** – Port status is disabled.
Port Use
Possible Settings: **Frame Relay, Synchronous Data** Default Setting: **Frame Relay** when the port supports frame relay. **Synchronous Data** when the port only supports synchronous data.
Determines how the data port will be used. *Display Conditions* – This option only appears for user data on Port-2. **Frame Relay** – The port is configured for frame relay traffic. Frame relay links, DLCis, and PVC connections can be configured on this port. **Synchronous Data** – The port is configured for standard TDM data, and can be cross-connected to a time slot on a T1 interface. ■ No alarms or traps configured for the port will be generated. ■ The LED for the port will be held in an Off state. ■ Existing cross-connect assignments associated with the port are cleared.

Table 4-7. Data Port Physical Interface Options (2 of 5)

Max Port Rate (Kbps)
Possible Settings: **1536, 2048** Default Setting: **1536**
Specifies the maximum clock rate for a user data port. The data rate for this port is limited to the rate specified by this option so that the maximum rate supported by an attached DTE is not exceeded. *Display Conditions* – This option only appears when the Port Use is set to Frame Relay and, if the unit has multiple data ports, the selected port is Port-2. **1536** – The maximum port rate for the port is 1536 Kbps. **2048** – The maximum port rate for the port is 2048 Kbps.
Port Base Rate (Kbps)
Possible Settings: **Nx64, Nx56** Default Setting: **Nx64**
Specifies the base rate for the data port, which is a multiple (from 1 to 24) of the base rate specified by this option. N is a number from 1 to 24. *Display Conditions* – This option only appears when Port Use is set to Synchronous Data. This option does not appear for a FrameSaver SLV 9128-II. **Nx64** – The base rate for the port is 64 Kbps. **Nx56** – The base rate for the port is 56 Kbps.
Invert Transmit Clock
Possible Settings: **Auto, Enable, Disable** Default Setting: **Auto**
Determines whether the clock supplied by the FrameSaver unit on interchange circuit DB (ITU 114) – Transmit Signal Element Timing (DCE Source) TXC is phase inverted with respect to the clock used to time the incoming Transmitted Data (TD). **Auto** – The port checks the clock supplied by the DCE on TXC on this port. If necessary, the port automatically phase inverts the clock with respect to the transmitted data. **Enable** – Phase inverts the TXC clock. Use this setting when long cable lengths between the FrameSaver unit and the DTE are causing data errors. **Disable** – Does not phase invert the TXC clock.
Transmit Clock Source
Possible Settings: **Internal, External** Default Setting: **Internal**
Determines whether the DTE's transmitted data is clocked into the FrameSaver unit by its internal transmit clock or by the external clock provided by the DTE. NOTE: Changing settings for this configuration option causes the FrameSaver unit to abort any physical port tests, including any DTE-initiated loopback tests. **Internal** – The FrameSaver unit uses the interchange circuit DB (ITU 114) – Transmit Signal Element Timing (TXC) (DCE source) for timing the incoming data. **External** – The DTE provides the clock for the transmitted data, and the FrameSaver unit uses the interchange circuit DA (ITU 113) – Transmit Signal Element Timing (XTXC) (DTE source) for timing the incoming data.

Table 4-7. Data Port Physical Interface Options (3 of 5)

Monitor RTS (Control)
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the Request To Send (RTS) circuits on the user data port will be used to determine when valid data communication is possible with the DTE. When this condition is detected, CTS is deasserted, LMI is declared down, and no further transfer of frame relay data can occur on this interface. **Enable** – Interchange circuit CA (ITU 105) – RTS is monitored to determine when valid data communication is possible with the DTE. **Disable** – RTS is not monitored. RTS is assumed to be asserted and data is being transmitted, regardless of the state of the lead.
Monitor DTR
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the state of the DTE Ready (DTR) circuit on the user data port will be used to determine when valid data communication is possible with the DTE. When this condition is detected, an alarm is generated, LMI is declared down, and no further transfer of frame relay data can occur on this interface. **Enable** – Interchange circuit CD (ITU 108/1/2) – DTR is monitored to determine whether data should be transmitted to the DTE. **Disable** – DTR is not monitored. DTR is assumed to be asserted and data is being transmitted, regardless of the state of the lead.

Table 4-7. Data Port Physical Interface Options (4 of 5)

Port (DTE) Initiated Loopbacks
Possible Settings: *When Port-1 or Port Use is set to Frame Relay:* **Disable**, **Local** *When Port-2 or Port Use is set to Synchronous Data:* **Disable**, **DTPLB, DCLB, Both** Default Setting: **Disable**
Possible Settings: **Local**, **Disable** Default Setting: **Disable**
When Port-1 or Port Use is set to Frame Relay: Allows a local external DTE Loopback to be started or stopped via the data terminal equipment attached to the port's interchange lead LL (ITU 141), as specified by V.54. **Disable** – The DTE attached to the port cannot control the local external DTE Loopback. **Local** – The DTE attached to the port controls the local external DTE Loopback. ***When Port-2 or Port Use is set to Synchronous Data:*** Allows local Data Terminal Loopbacks (DTPLBs) and remote Data Channel Loopbacks (DCLBs) to be controlled by the DTE connected to this port. *Display Conditions* – This option does not appear when Port Type is set to X.21. **Disable** – The DTE attached to the port cannot control Local Data Terminal Loopbacks (DTPLBs) and remote Data Channel Loopbacks (DCLBs). **DTPLB** – The DTE attached to the port controls DTPLBs via circuit LL – CCITT 141, as specified by V.54. The port remains in loopback as long as the circuit stays on. **DCLB** – The DTE attached to the port controls DCLBs via circuit RL – CCITT 140, as specified by V.54. The far-end equipment must support inband V.54 loopbacks. **Both** – The DTE attached to the port controls both local DTPLBs and remote DCLBs.
Invert Transmit and Receive Data
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether transmitted and received data for the synchronous data port is logically inverted before being transmitted or after being received from the network. Use this configuration option for applications where data is being transported using HDLC protocol, whereby inverting the data ensures that the ones density requirements for the network are met. *Display Conditions* – This option only appears for Port-2 on a FrameSaver SLV 9128-II, when Port Use is set to Synchronous Data. **Enable** – Inverts the transmitted and received data for the port. **Disable** – Does not invert the transmitted and received data for the port.

Table 4-7. Data Port Physical Interface Options (5 of 5)

Action on Network Yellow Alarm
Possible Settings: **None, Halt** Default Setting: **Halt**
Specifies the action to take on the synchronous data port when a yellow alarm is received on the network interface. (A yellow alarm indicates a problem with the signal being transmitted to the network.) *Display Conditions* – This option only appears for Port-2 on a FrameSaver SLV 9128-II, when Port Use is set to Synchronous Data. **None** – No action taken when a yellow alarm is received. **Halt** – Halts the transmission of data received on the synchronous data port and all ones are sent on circuit BB (ITU 104) – Receive Data (RD) and circuit CB (ITU 106) – Clear-to-Send (CTS) is deasserted to the port when a yellow alarm is received.
Network Initiated Data Channel Loopback
Possible Settings: **Disable, V.54, ANSI_FT1, V.54_&_ANSI** Default Setting: **Disable**
Allows the initiation and termination of the Data Channel Loopback (V.54 Loop 2) to be controlled by the receipt of a DCLB-actuate and DCLB-release sequence (either V.54, or FT1 [ANSI] compliant sequences) from the network or far end unit. When this configuration is enabled (V.54, FT1, or Both), receiving a DCLB-actuate sequence on a particular port causes the unit to initiate a DCLB on that port (provided that a DCLB can be performed based on the current state of the port and unit). Receiving a DCLB-release sequence terminates the DCLB. *Display Conditions* – This option only appears for Port-2 on a FrameSaver SLV 9128-II, when Port Use is set to Synchronous Data. **Disable** – Ignores the DCLB-actuate and DCLB-release for the port. **V.54** – DCLB-actuate and DCLB-release sequences that comply with the V.54 standard for “inter-DCE signaling for point-to-point circuits” are recognized and will control the initiation and termination of a DCLB (V.54 Loop 2) for the port. **ANSI_FT1** – DCLB-actuate and DCLB-release sequences that comply with either the ANSI.403, Annex B standard for “in-band signaling for fractional T1 (FT1) channel loopbacks” are recognized and will control the initiation and termination of a DCLB for the port. **V.54_&_ANSI** – DCLB-actuate and DCLB-release sequences that comply with either the ANSI or V.54 standard are recognized and will control the initiation and termination of a DCLB for the port.

Configuring the DSX-1 Interface

Select DSX-1 to display or change the physical configuration options when a DSX-1 interface is installed (see Table 4-8, DSX-1 Physical Interface Options).

Main Menu→Configuration→DSX-1

Table 4-8. DSX-1 Physical Interface Options (1 of 2)

Interface Status
Possible Settings: **Enable, Disable** Default Setting:**Disable**
Specifies whether the DSX-1 interface selected is available for use. **Enable** – The interface is available. **Disable** – The interface is not available for use. If there are time slots assigned to the DSX-1 interface when you attempt to disable it, the message **`This action will clear all DSX-1 Cross Connections. Are You Sure? No`** appears. If you select: **No** – The operation is cancelled. **Yes** – The following occurs: ■ All existing DSX-1 interface cross-connect assignments are cleared. ■ Alarms or traps associated with the DSX-1 interface are not generated. ■ LEDs associated with the DSX-1 interface are held in an “off’’ state.
Line Framing Format
Possible Settings: **D4, ESF** Default Setting: **ESF**
Specifies the framing format for transmitted and received signals on the DSX-1 interface. **D4** – Uses D4 framing format. **ESF** – Uses Extended Superframe (ESF) framing format.
Line Coding Format
Possible Settings: **AMI, B8ZS** Default Setting: **B8ZS**
Specifies the line coding format for the DSX-1 interface. **AMI** – Uses Alternate Mark Inversion (AMI) line coding format. **B8ZS** – Uses Bipolar 8 Zero Substitution (B8ZS) line coding format.

Table 4-8. DSX-1 Physical Interface Options (2 of 2)

Line Equalization
Possible Settings: **0–133, 133–266, 266–399, 399–533, 533–655** Default Setting: **0–133**
Permits a standard DSX signal to be delivered over a distance of up to 655 feet. **0–133** – Equalization on the DSX-1 side allows up to 133 feet of cable between the FrameSaver unit and the DTE. **133–266** – Equalization on the DSX-1 side allows up to 266 feet of cable between the FrameSaver unit and the DTE. **266–399** – Equalization on the DSX-1 side allows up to 399 feet of cable between the FrameSaver unit and the DTE. **399–533** – Equalization on the DSX-1 side allows up to 533 feet of cable between the FrameSaver unit and the DTE. **533–655** – Equalization on the DSX-1 side allows up to 655 feet of cable between the FrameSaver unit and the DTE.
Send All Ones on DSX-1 Failure
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether action is taken when a valid signal cannot be recovered for the DSX-1 (LOS, continuous OOF, or AIS). **Enable** – Sends all ones on the DS0 channels allocated to the DSX-1 interface in the event of an LOS, AIS, or continuous OOS condition on the DSX-1 interface. **Disable** – No action is taken when a signal fails on the DSX-1 interface. The data received is passed through the network interface channels unchanged.

Configuring the ISDN DBM Interface

For models with ISDN backup capability, select Physical from the ISDN menu to configure the physical characteristics for DBM Interface.

Main Menu→Configuration→ISDN→Physical

When configuring a BRI DBM, refer to Table 4-9, ISDN BRI DBM Physical Interface Options.

When configuring a PRI DBM, refer to Table 4-10, ISDN PRI DBM Physical Interface Options.

Table 4-9. ISDN BRI DBM Physical Interface Options

Interface Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the ISDN interface is available for use. **Enable** – The ISDN interface is enabled. **Disable** – The ISDN interface cannot be configured, nor can it transmit or receive data. No PVC connections or frame relay DLCIs will be deleted. Disabling the ISDN interface results in the following: ■ All currently connected ISDN calls are terminated. ■ Alarms or traps associated with this interface are not generated or displayed.
Service Profile ID (SPID) 1 or 2
Possible Settings: **3 – 20 digits** Default Setting: **Clear**
Specifies the SPID number assigned by the ISDN service provider for Bearer channel 1 (B1) and Bearer channel 2 (B2). SPID numbers are used by the switch to identify which ISDN services the DBM can access. All blanks is a valid setting. **3 – 20 digits** – You can enter a SPID number, or you can leave blanks. If a nondigit/numeric is entered, an **`Invalid Character (x)`** message appears at the bottom of the screen. If fewer than three digits/numerics are entered, an **`Invalid – SPID must be at least 3 digits`** message appears at the bottom of the screen. **Clear** – Clears the SPID field so it can be reentered.
Local Phone Number 1 or 2
Possible Settings: **10 digits** Default Setting: **Clear**
Provides the telephone number associated with Bearer channel 1 (B1) and 2 (B2). All blanks is a valid setting. **10 digits** – Enter the telephone number, up to 10 digits. If a nondigit/numeric is entered, an **`Invalid Character (x)`** message appears at the bottom of the screen. **Clear** – Clears the phone number field so it can be reentered.

Refer to the Table 4-10 when configuring a PRI DBM.

Table 4-10. ISDN PRI DBM Physical Interface Options (1 of 3)

Interface Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the ISDN interface is available for use. **Enable** – The ISDN interface is enabled. **Disable** – The ISDN interface cannot be configured, nor can it transmit or receive data. No PVC connections or frame relay DLCIs will be deleted. Disabling the ISDN interface results in the following: ■ All currently connected ISDN calls are terminated. ■ Alarms or traps associated with this interface are not generated or displayed. ■ LEDs associated with this interface are held in an “off" state. Specifically, the DSX/PRI LEDs are held off if they represent the PRI status.
Switch Type
Possible Settings: **NI-2, ATT_4ESS, ATT_5ESS** Default Setting: **NI-2**
Specifies type of ISDN switch provided by the server. **NI-2** – The DBM will communicate with a service provider supporting the National ISDN-2 switching standard. **ATT_4ESS** – The DBM will communicate with a service provider supporting the ATT 4ESS switching standard. **ATT_5ESS** – The DBM will communicate with a service provider supporting the ATT 5ESS switching standard.
Local Phone Number
Possible Settings: **10 digits** Default Setting: **Clear**
Provides the telephone number associated with all Bearer channels. All blanks is a valid setting. **10 digits** – Where you enter the telephone number, up to 10 digits. If a nondigit/numeric is entered, an **`Invalid Character (x)`** message appears at the bottom of the screen. **Clear** – Clears the phone number field so it can be reentered.
Line Framing Format
Possible Settings: **D4, ESF** Default Setting: **ESF**
Specifies the framing format for transmitted and received signals on the ISDN interface. **D4** – Uses D4 framing format. NOTE: This setting is not recommended by network carriers. False yellow alarms may occur after traffic has been running and the channel returns to idle, or when there is light traffic when other settings are selected. ESF format does not create this problem. **ESF** – Uses Extended Superframe framing format.

Table 4-10. ISDN PRI DBM Physical Interface Options (2 of 3)

Line Build Out (LBO)
Possible Settings: **0.0, –7.5, –15, –22.5** Default Setting: **0.0**
Specifies the line build out for the signal transmitted to the ISDN. **0.0, –7.5, –15, –22.5** – Specifies line build out in dB.
Network Initiated LLB
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Allows the initiation and termination of the line loopback (LLB) to be controlled by the receipt of LLB-Actuate and LLB-Release commands from the ISDN. **Enable** – LLB is controlled by LLB-Actuate and LLB-Release commands. Receiving a LLB-Actuate command causes the system to enter a line loopback (provided an LLB can be performed in the system's current state). Receiving an LLB-Release command terminates the LLB. **Disable** – The system ignores the LLB-Actuate and LLB-Release commands. NOTE: When disabled, the system is not in compliance with ANSI T1.403 or AT&T TR 62411.
Network Initiated PLB
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Allows the initiation and termination of the payload loopback (PLB) to be controlled by the receipt of PLB-Actuate and PLB-Release commands from the ISDN. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **Enable** – PLB is controlled by PLB-Actuate and PLB-Release commands. Receiving a PLB-Actuate command causes the system to enter a payload loopback (provided a PLB can be performed in the system's current state). Receiving a PLB-Release command terminates the PLB. **Disable** – The system ignores the PLB-Actuate and PLB-Release commands. NOTE: When disabled, the unit is not in compliance with ANSI T1.403 or AT&T TR 54016.
ANSI Performance Report Messages
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether ANSI T1.403 compliance performance report messages (PRMs) are generated and sent to the ISDN over the ESF facility data link every second. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **Enable** – Generates and sends PRMs. **Disable** – Does not generate and send PRMs.

Table 4-10. ISDN PRI DBM Physical Interface Options (3 of 3)

Excessive Error Rate Threshold
Possible Settings: **10E-4, 10E-5, 10E-6, 10E-7, 10E-8, 10E-9** Default Setting: **10E-4**
Sets the error rate threshold that determines when an EER condition is declared. The excessive error rate is determined by the ratio of the number of CRC6 errors to the total number of bits received over a set period of time. *Display Conditions* – This option only appears when Line Framing Format is set to ESF. **10E-4** – Declares an EER if more than 1,535 CRC6 errors are detected in a 10 second period. Clears when fewer than 1,536 CRC6 errors are detected within the same time period. **10E-5** – Declares an EER if more than 921 CRC6 errors are detected in a 60 second period or a 10^{-4} condition occurs. Clears when fewer than 922 CRC6 errors are detected within the same time period. **10E-6** – Declares an EER if more than 92 CRC6 errors are detected in a 60 second period or a 10^{-5} or 10^{-4} condition occurs. Clears when fewer than 93 CRC6 errors are detected within the same time period. **10E-7** – Declares an EER if more than 9 CRC6 errors are detected in a 60 second period or a 10^{-6}, or 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 10 CRC6 errors are detected within the same time period. **10E-8** – Declares an EER if more than 41 CRC6 errors are detected in three 15 minute intervals or a 10^{-7}, 10^{-6}, 10^{-5}, 10^{-4} condition occurs. Clears when fewer than 42 CRC6 errors are detected within the same time period. **10E-9** – Declares an EER if more than 4 CRC6 errors are detected in three 15 minute intervals or a 10^{-8}, 10^{-7}, 10^{-6}, 10^{-5}, or 10^{-4} condition occurs. Clears when fewer than 5 CRC6 errors are detected within the same time period.
Circuit Identifier
Possible Settings: ***ASCII Text Entry*, Clear** Default Setting: **blank**
Identifies the transmission vendor's circuit information to facilitate troubleshooting. ***ASCII Text Entry*** – Assigns a name to identify the circuit (maximum 255 characters). **Clear** – Removes the circuit identifier information.

Setting Up ISDN Link Profiles

For models with ISDN backup capability, select ISDN Link Profiles from the ISDN menu to set up the ISDN Link Profiles (see Table 4-11, ISDN Link Profile Options).

Main Menu→Configuration→ISDN→ISDN Link Profiles

Table 4-11. ISDN Link Profile Options (1 of 3)

Link Name
Possible Settings: ***ASCII Text Entry*, HQ_Site** Default Setting: **HQ_Site** for first link; blank for all others
Assigns the name to the ISDN link profile. It is generally the backup destination for a frame relay link. Each profile must have a unique link name. If the link name field is blank, the link profile will be deleted. Use ASCII text, 8 characters maximum. ***ASCII Text Entry*** – Assigns a name to identify the ISDN link (maximum 255 characters). NOTE: To prevent confusion, do not use the following link names: Network, Net1-FR1, Port-1, or Port-2. These names will be treated as nonunique and the **`Link Name Not Unique`** message appears and you must enter another name. **HQ_Site** – The link name configured in the remote site unit (originating a backup call) for the central site unit (answering a backup call). One link has a default value of HQ_Site to allow for Automatic Backup Configuration.
Link Status
Possible Settings: **Auto, Disable** Default Setting: **Auto**
Determines whether the ISDN frame relay link is in or out of service. **Auto** – The link is configured to be in service when needed. Packets will be transmitted and received on the interface, and the LMI for a PVC connection will become active when the link is required. If this profile is configured as the alternate link and the primary link or DLCI fails, the unit dials the Outbound Phone Number, or the Alternate Outbound Phone Number if the first call was unsuccessful. The unit also answers calls from Inbound Call IDs associated with this link. This link profile becomes active when: ■ This profile is configured as the alternate link and there is a failure of a primary link or DLCI. ■ Source or Primary Destination DLCIs are configured on this link. When the primary link recovers, the call is automatically disconnected. **Disable** – The frame relay link is out of service. No data will be transmitted or received on the interface. If there is are any active calls when disabled, the calls are ended and no calls will be answered or originated using this profile.

Table 4-11. ISDN Link Profile Options (2 of 3)

Outbound Phone Number

Possible Settings: **0 – 9**, *****, **#**, space, _ , **–**, (, or)
Default Setting: none

Specifies the primary phone number to call (the ISDN Called Party Identifier) for the Link Profile. Up to 18 valid characters can be entered. Each Outbound Phone Number must be unique. If not, the **`Outbound Phone Number is Not Unique`** message appears and you must enter another phone number.

> NOTE: For every originating (outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa.

Currently active calls are not effected when this number is changed.

Inbound Calling ID 1 or 2

Possible Settings: **0** – **9**
Default Setting: none

Specifies the local phone number of a remote device from which that the unit will accept calls (the ISDN Calling Party Identifier). Up to 18 digits can be entered. Each Inbound Calling ID must be unique. If not, the **`Inbound Calling ID`** ***`n`*** **`is Not Unique`** message appears and you must enter another phone number.

For remote devices with a PRI DBM, only one Inbound Calling ID is required. Inbound Calling ID 2 is provided to identify incoming calls from a second phone number assigned to a remote device with a BRI DBM.

NOTES:

- Inbound Calling ID 2 is only useful when multiple local phone numbers are programmed at the originating site (e.g., a 2B+D BRI location).
- For every originating (outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa.

Currently active calls are not effected when this number is changed.

0 – 9 – Specifies the numbers in the remote device's local phone number.

Maximum Link Rate (Kbps)

Possible Settings:
For a BRI DBM: **64**, **128**
For a PRI DBM: **64** – **1472**

Default Setting: **64**

Specifies the maximum rate that will be attempted for the frame relay link when it is activated. The actual rate achieved on the link depends upon the number of successful calls placed or answered, and the negotiated rate on each call.

> NOTE: This option takes effect as soon as a change is saved. If the rate is increased, additional calls will be placed. If the rate is decreased, calls will be dropped. For extra calls to be successful, the Maximum Link Rate must be increased at the originating device before it is increased at the answering device.

64 – An individual frame relay link is formed and a single call is placed using a B-channel when the link is activated.

128 . . . 1472 – A constituent link is configured for each multiple of 64 Kbps in the specified bandwidth. This bundle of constituent links will function as a single frame relay multilink. When the multilink aggregate link is activated, calls will be placed or answered on as many constituent links as possible based upon available B-channels.

Table 4-11. ISDN Link Profile Options (3 of 3)

Caller Identification Method
Possible Settings: **Caller ID**, **Proprietary** Default Setting: **Caller ID**
Specifies the method used to identify callers. NOTE: The Caller Identification Method setting must be the same at both ends of the circuit. **Caller ID** – Incoming calls will only be answered and the frame relay link on this Link Profile will only be activated when the Caller ID received from the switch matches one of the configured Inbound Calling IDs. **Proprietary** – Incoming calls will always be answered, even when no Caller ID is provided by the switch, provided the following conditions are met: ■ Link Status is set to Auto (the default). ■ At least one ISDN Link Profile is enabled. When using the Proprietary method, the unit queries the originating unit for its Local Phone Number. If the returned phone number matches one of the configured Inbound Calling IDs, the call is accepted. If the queried unit does not respond with its phone number within five seconds, the unit drops the call.
Alternate Outbound Phone Number
Possible Settings: **0 – 9**, *****, **#**, space, _ , **–**, (, or) Default Setting: none
Specifies an alternate phone number to call (the ISDN Called Party Identifier) when a call using the primary Outbound Phone Number was unsuccessful. Up to 18 valid characters can be entered. Each Outbound Phone Number must be unique. If not, the **`Alt Outbound Phone Number is Not Unique`** message appears and you must enter another phone number. NOTE: For every originating (alternate outbound) phone number entered, an answering (inbound) phone number must be entered at the far end, and vice versa. Currently active calls are not effected when this number is changed.

Assigning Time Slots/Cross Connections

The Time Slot Assignment/Cross Connect feature provides an easy method of assigning time slots for frame relay data and creating cross-connections to the synchronous data interface. The system allows you to assign DS0s on the T1 network interface and between the user data port and network interface in order to share the T1 network.

You can also clear cross-connection assignments for the system, or for a selected slot or interface.

NOTE:

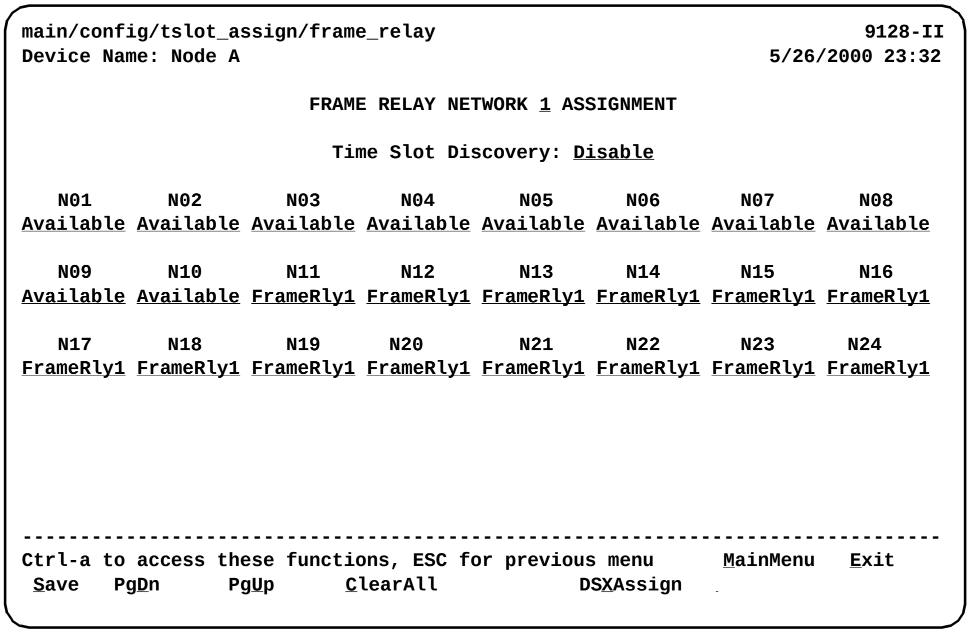
Although it is not required, it is suggested that you progress through each screen in order, from top to bottom.

Assigning Frame Relay Time Slots to the Network Interface

Before assigning network time slots for use by frame relay traffic, configure the Network physical and Frame Relay options (if needed), then allow Time Slot Discovery to autodetect and assign the appropriate time slots to frame relay.

If there are multiple Frame Relay data links on the network interface, or if Time Slot Discovery is not currently active, you can manually assign time slots on the network interface for frame relay traffic using the Frame Relay Network Assignments screen. This screen is read-only when Time Slot Discovery is set to Enable for the network interface.

Frame Relay Network Time Slot Assignment Screen Example



```
main/config/tslot_assign/frame_relay                                    9128-II
Device Name: Node A                                                5/26/2000 23:32

                         FRAME RELAY NETWORK 1 ASSIGNMENT

                           Time Slot Discovery: Disable

   N01      N02       N03       N04       N05      N06       N07       N08
Available Available Available Available Available Available Available Available

   N09      N10       N11       N12       N13      N14       N15       N16
Available Available FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1

   N17      N18       N19      N20        N21      N22       N23      N24
FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1






--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save   PgDn      PgUp      ClearAll            DSXAssign
```

Value	Meaning
Time Slot Discovery	Specifies whether the time slots used for frame relay traffic should be discovered from the network interface upon detection of an LMI failure. This option allows additional time slots to be added without manually reconfiguring the device.
N *tt*	This field represents time slot *tt* of the selected network interface.
Assigned	The time slot is already assigned to something other than frame relay, so it is unavailable. Assigned time slots cannot be modified from this screen.
Available	The time slot is currently unassigned.
FrameRly1	The time slot is assigned to frame relay service, link 1.

For easy movement between screens, select the DSXAssign function key to go directly to the DSX-1 to Network Assignments screen.

Time Slot Assignment Rule:

Valid network time slots are either **Available** or contain a Frame Relay Link 1 assignment.

▶ Procedure

1. Follow this menu selection sequence:

   Main Menu→Configuration→Time Slot Assignment →
   Frame Relay Network Assignments

   The Frame Relay Network Assignments screen appears. This screen contains a matrix of the current assignment status of all time slots on the network interface.

2. Enable or disable Time Slot Discovery.

   — When enabled, the unit examines all time slots not cross-connected to other ports to determine which time slots are being used by the network for frame relay traffic. These time slots are set to **FrameRly1**. This is the factory default.

   — When disabled, time slot assignments must be manually configured.

3. If Time Slot Discovery is disabled, assign network time slots for use by frame relay service, link 1, by typing **FrameRly1** in the selected Network field.

4. Repeat Step 3 until all desired time slots are assigned.

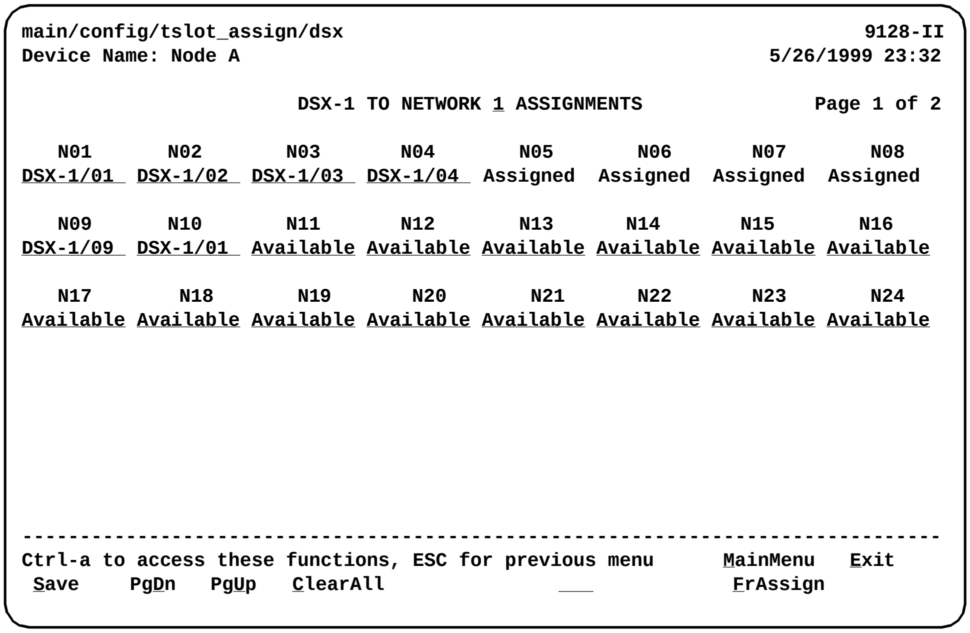
5. Save the configuration.

Assigning DSX-1 Time Slots to the Network Interface

DSX-1 time slots are assigned by channel allocation, where you specify individual time slots. The DSX-1 interface must be enabled to assign DSX-1 time slots to the network interface (see Table 4-8, DSX-1 Physical Interface Options).

Value	**Meaning**
N*tt*	It represents time slot *tt* of the selected network interface.
Assigned	The time slot is already assigned to something other than a DSX-1 time slot, so it is unavailable. Assigned time slots cannot be modified from this screen.
Available	The time slot is currently unassigned.
DSX-1/*tt*	Slot *tt* of the DSX-1 interface is assigned to the network interface time slot identified right above it (N*tt*).

DSX-1 to Network Time Slot Assignment Screen Example (Page 1)



```
main/config/tslot_assign/dsx                                           9128-II
Device Name: Node A                                            5/26/1999 23:32

                       DSX-1 TO NETWORK 1 ASSIGNMENTS              Page 1 of 2

   N01       N02       N03       N04       N05       N06       N07       N08
DSX-1/01  DSX-1/02  DSX-1/03  DSX-1/04  Assigned  Assigned  Assigned  Assigned

   N09       N10       N11       N12       N13       N14       N15       N16
DSX-1/09  DSX-1/01  Available Available Available Available Available Available

   N17       N18       N19       N20       N21       N22       N23       N24
Available Available Available Available Available Available Available Available








--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu       MainMenu   Exit
 Save     PgDn   PgUp   ClearAll               ___          FrAssign
```

Page 2 of 2 is for defining signaling assignments and trunk conditioning for each DSX-1 interface time slot. See *DSX-1 Signaling Assignments and Trunk Conditioning (Page 2)* on page 4-55 for an example of this screen.

For easy movement between screens, select the FrAssign function key to go directly to the Frame Relay Network Assignments screen.

Time Slot Assignment Rules:

- Valid Network time slots are either **Available** or contain a DSX-1 time slot assignment.
- Valid DSX-1 time slots are those that are unassigned, including the currently assigned time slot.
- Order of display is as follows:
  - — **Available** is the first selection.
  - — Then, from the lowest DSX-1 interface to the highest DSX-1 interface.
  - — Then the lowest available time slot number to the highest available time slot number.

  For example, if the cursor is on a field with the **Available** value under assigned time slot N*tt*, pressing the Spacebar causes this field's values to cycle through all valid DSX-1 time slots, starting with D*s*-*p*/*yy*, assuming it is unassigned. If D*s*-*p*/*tt* is already assigned, the next valid time slot in the order described above is displayed.

▶ Procedure

1. Follow this menu selection sequence:

   Configuration→Time Slot Assignment→DSX-to-Network Assignments

   The DSX-1 to Network Assignments screen appears. This screen contains a matrix of the current cross-connect status of all time slots on the network interface.

2. Move the cursor to the next time slot that can be edited (underlined). Use the spacebar or type in the desired time slot to display its time slot assignment.

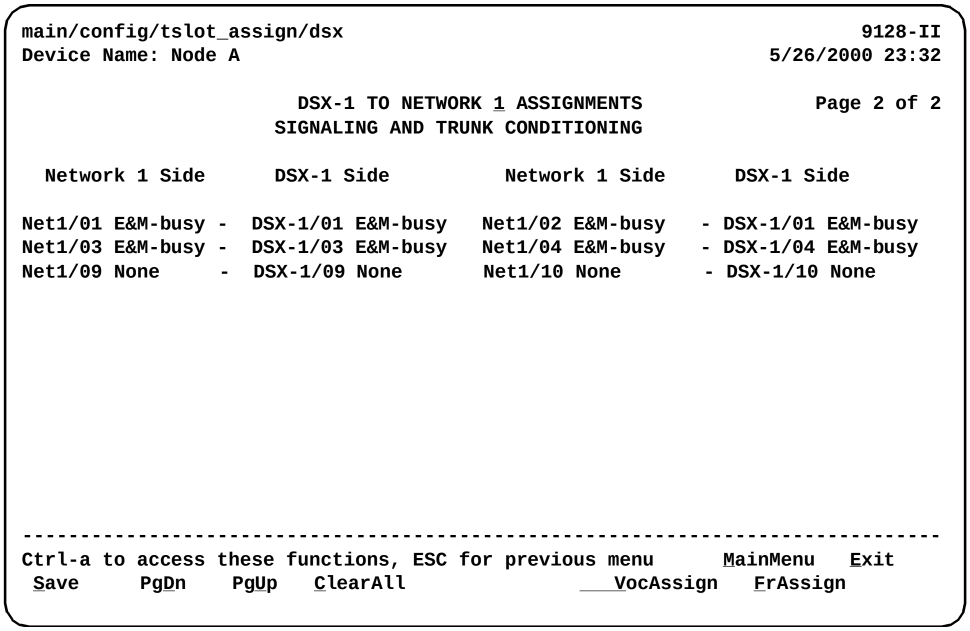
3. Repeat Step 2 until all desired time slots are assigned.

4. Save the configuration.

DSX-1 Signaling Assignments and Trunk Conditioning (Page 2)

The second page of the DSX-1 to Network Assignments screen allows you to define the signaling assignments and trunk conditioning for each time slot on the DSX-1 interface. You can specify whether robbed bit signaling information is being passed within a given DS0, and the value of the signaling bits that will be transmitted for that DS0 to the other cross-connected T1 network interface if a Carrier Group Alarm (CGA) occurs on a T1 network interface.

DSX-1 to Network Time Slot Assignment Screen Example (Page 2)



```
main/config/tslot_assign/dsx                                           9128-II
Device Name: Node A                                            5/26/2000 23:32

                       DSX-1 TO NETWORK 1 ASSIGNMENTS              Page 2 of 2
                     SIGNALING AND TRUNK CONDITIONING

  Network 1 Side      DSX-1 Side          Network 1 Side      DSX-1 Side

Net1/01 E&M-busy -  DSX-1/01 E&M-busy   Net1/02 E&M-busy   - DSX-1/01 E&M-busy
Net1/03 E&M-busy -  DSX-1/03 E&M-busy   Net1/04 E&M-busy   - DSX-1/04 E&M-busy
Net1/09 None     -  DSX-1/09 None       Net1/10 None       - DSX-1/10 None










-------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save     PgDn    PgUp   ClearAll               ___VocAssign   FrAssign
```

For easy movement between screens, select the FrAssign function key to go directly to the Frame Relay Network Assignments screen or the DSXAssign function key to go to the DSX-1 to Network Assignments screen.

Only those DSX-1-to-Network assignments from page 1 are displayed on this page, from left to right and top to bottom in ascending order, by network and time slot.

When a CGA condition (LOS, OOF, or AIS) is declared for a T1 interface, the signaling bits being transmitted to the other T1 interface for the DS0 are forced to idle for two seconds (except for user-defined patterns which are transmitted immediately). This drops any call in progress. The signaling bits are then forced to the selected state (Busy or Idle), and remain in this state until the CGA condition clears. At this point, the received signaling bits from the T1 interface which formerly had the CGA condition are passed through to the other T1 interface.

NOTE:

Trunk conditioning will only occur on DS0s that are cross-connected to another T1 interface. All other DS0s remain unaffected by trunk conditioning.

Enter one of the values shown in Table 4-12, Signaling and Trunk Conditioning Values, in each of the fields on both the Network side and the DSX-1 side. Although you can choose any value for the DSX-1 side, the default value displayed is based on a typical setting that would be used with the corresponding Network side value. Typical pairs of values are shown in the table below. If you change the Network side value, the DSX side value is changed to the corresponding default value.

Table 4-12. Signaling and Trunk Conditioning Values (1 of 3)

Network Side	Meanings	DSX-1 Side
None	No signaling used on this DS0. Use this setting if there is no voice signaling information being passed on this DS0 (clear channel).	None
RBS (default)	Robbed Bit Signaling is used on this DS0, but no trunk conditioning. Signaling bits will be passed to the T1 interface to which this DS0 is cross-connected when this T1 interface is not in CGA, but the signaling bits will be all ones when CGA is present.	RBS
The following values configure the cross-connect for RBS, as well as perform the trunk conditioning. Although ABCD signaling bits for each setting are described, only AB bits are transmitted when the cross-connected T1 network interface is using D4 framing.		

Table 4-12. Signaling and Trunk Conditioning Values (2 of 3)

Network Side	Meanings	DSX-1 Side
E&M-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an E&M interface (ABCD = 0000).	E&M idle
E&M-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an E&M interface (ABCD = 1111).	E&M busy
FXOg-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXO Ground-Start interface (ABCD = 1111).	FXSg-idle
FXOg-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXO Ground-Start interface (ABCD = 0101).	FXSg-busy
FXOl-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXO Loop-Start interface (ABCD = 0101).	FXSl-idle
FXOl-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXO Loop-Start interface (ABCD = 0101).	FXSl-busy
FXSg-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXS Ground-Start interface (ABCD = 0101).	FXOg-idle
FXSg-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXS Ground-Start interface (ABCD = 1111).	FXOg-busy
FXSl-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXS Loop-Start interface (ABCD = 0101).	FXOl-idle
FXSl-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXS Loop-Start interface (ABCD = 1111).	FXOl-busy
FXOD-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXODN interface (ABCD = 0000).	FXSD-idle
FXOD-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXODN interface (ABCD = 1111).	FXSD-busy
FXSD-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for an FXSDN interface (ABCD = 0000).	FXOD-idle
FXSD-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an FXSDN interface (ABCD = 1111).	FXOD-busy

Table 4-12. Signaling and Trunk Conditioning Values (3 of 3)

Network Side	Meanings	DSX-1 Side
PLAR3idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a PLAR D3 interface (ABCD = 0000).	PLAR3idle
PLAR3busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an PLAR D3 interface (ABCD = 1111).	PLAR3busy
PLAR4idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a PLAR D4 interface (ABCD = 1111).	PLAR4idle
PLAR4busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for an PLAR D4 interface (ABCD = 0000).	PLAR4busy
DPO-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a DPO interface (ABCD = 0000).	DPT-idle
DPO-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for a DPO interface (ABCD = 1111).	DPT-busy
DPT-idle	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the idle state for a DPT interface (ABCD = 0000).	DPO-idle
DPT-busy	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent the busy state for a DPT interface (ABCD = 1111).	DPO-busy
USER-*xxxx*	The signaling bits transmitted to the cross-connected T1 interface during a CGA represent a user-defined pattern of ABCD = *xxxx*.	USER-*xxxx**

* *xxxx* is the same value on both the Network and the DSX-1 sides.

Assigning a Synchronous Data Port to Network or DSX-1 Time Slots

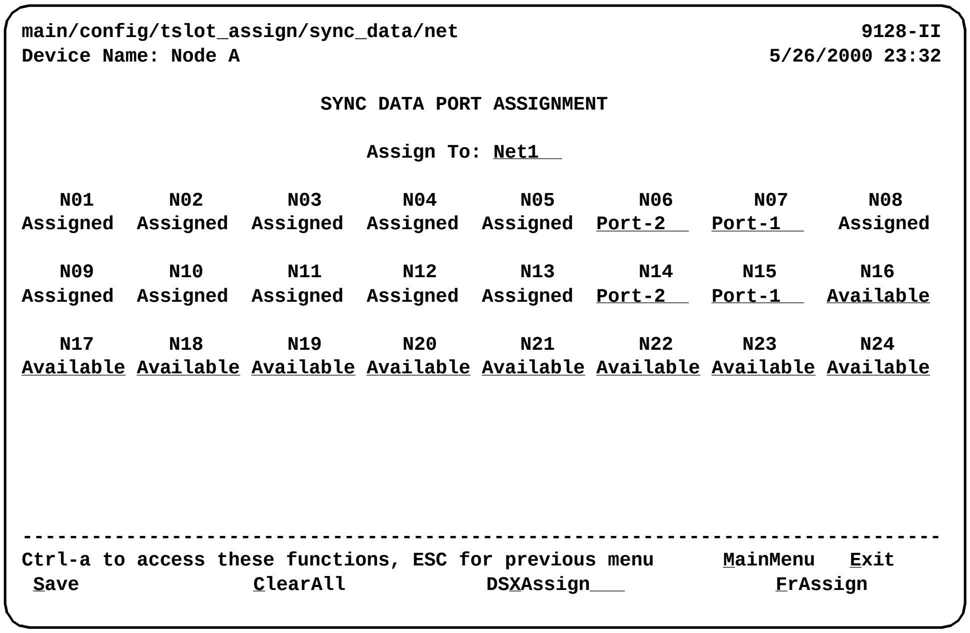
For a FrameSaver SLV 9128-II, which has two data ports, another assignment screen is available. Use the Sync Data Port Assignment screen to view the status of:

- All DS0 assignments on the Network interface
- All DS0 assignments on the DSX-1 interface

Then, you can a assign synchronous data port to:

- Network interface time slots
- DSX-1 interface time slots

Synchronous Data Port Assignment Screen Example



```
main/config/tslot_assign/sync_data/net                                  9128-II
Device Name: Node A                                              5/26/2000 23:32

                         SYNC DATA PORT ASSIGNMENT

                             Assign To: Net1

   N01      N02       N03       N04       N05       N06       N07       N08
Assigned Assigned  Assigned  Assigned  Assigned  Port-2    Port-1    Assigned

   N09      N10       N11       N12       N13       N14       N15       N16
Assigned Assigned  Assigned  Assigned  Assigned  Port-2    Port-1    Available

   N17      N18       N19       N20       N21       N22       N23       N24
Available Available Available Available Available Available Available Available






--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Save               ClearAll           DSXAssign             FrAssign
```

Value	Meaning
Assign To	Specifies either Net1 (network) or DSX1-1 (DSX-1) time slots.
N *tt* D *tt*	This field represents time slot *tt* of the network interface. This field represents time slot *tt* of the DSX-1 interface.
Assigned	The time slot is already assigned to a network or DSX-1 time slot. Assigned time slots cannot be modified from this screen.
Available	The time slot is currently unassigned.
Port-2	For a FrameSaver SLV 9128-II, synchronous data Port-2 is assigned to the time slot.

For easy movement between screens, select the FrAssign function key to go directly to the Frame Relay Network Assignments screen or the DSXAssign function key to go to the DSX-1 to Network Assignments screen.

Time Slot Assignment Rules:

- To assign a synchronous data port to network or DSX-1 time slots, Port-2's Port Use option must be set for Synchronous Data (see Table 4-7, Data Port Physical Interface Options).
- If the DSX-1 interface is disabled, only Net1 is available for synchronous data port assignment (see the Interface Status option in Table 4-8, DSX-1 Physical Interface Options).

▶ Procedure

1. Select one of the following menu selection sequences:

   Main Menu→Configuration→Time Slot Assignment →
   Sync Data Port Assignments or

   Main Menu→Easy Install→Time Slot Assignment Screen

2. Select an interface in the Assign To field. A matrix of the current cross-connect status of all time slots on the selected interface appears.
3. Move the cursor to the next time slot that can be edited (underlined). Use the spacebar or type in the desired time slot to display its time slot assignment.
4. Repeat Step 3 until the synchronous data port is assigned to all desired time slots.
5. Save the configuration.

Clearing Assignments

Clearing assignments sets all time slots to **Unassgn** (unassigned).

Main Menu→Configuration→Time Slot Assignment→Clear Assignments

Configuring Frame Relay for an Interface

Select Frame Relay from the interface's menu to display or change the Frame Relay options for an individual interface (see Table 4-13, Interface Frame Relay Options).

Main Menu→Configuration→[Network/Data Ports] →Frame Relay

See *Configuring Frame Relay for an Interface* on page 4-61, for additional information.

Table 4-13. Interface Frame Relay Options (1 of 3)

LMI Protocol
Possible Settings: **Initialize_From_Net1FR1**, **Initialize_From_Interface,** **Auto_On_LMI_Fail,** **Standard,** **Annex-A,** **Annex-D** Default Setting: *For a user data port link:* **Initialize_From_Interface** *For a network link:* **Auto_On_LMI_Fail**
Specifies either the LMI protocol supported on the frame relay interface or the discovery source for the LMI protocol. **Initialize_From_Net1FR1** – The LMI type supported on this frame relay link will be configured to match the LMI protocol initially discovered on the primary Network frame relay link (Net1FR1). LMI Protocol is set to None internally, but once a protocol has become active or is set on the primary Network link, the protocol will be set to the same value on this link (Standard, Annex-A or Annex-D). The protocol will *not* be updated based on changes to Net1FR1 after being set initially. *Display Conditions* – This option value only appears for a user data port. **Initialize_From_Interface** – The LMI type supported on this frame relay link will be configured to match the LMI protocol discovered from the attached Network line or DTE device. Once a protocol has become active, the protocol will be set to the protocol discovered (Standard, Annex-A or Annex-D) on the frame relay link. The protocol will *not* be updated after being initially discovered. Frame relay links on user data ports discover the LMI protocol from an attached device via LMI status polls. Frame relay links on the network interface discover LMI protocol by sending polls to an attached Network line and "listening" for correct poll response messages. **Auto_On_LMI_Fail** – The LMI type supported on this frame relay link will be configured to match the LMI protocol discovered from the attached Network line or the DTE device whenever an LMI Link Down failure occurs. This option is available for frame relay links on the Port and network interfaces. Frame relay links on user data ports discover the LMI protocol from LMI status polls by attached DTE devices. Frame relay links on the network interface discover LMI protocol by sending polls to an attached Network line and "listening" for correct poll response messages. **Standard** – Supports Standard LMI and the Stratacom enhancements to the Standard LMI. **Annex-A** – Supports LMI as specified by Q.933, Annex A. **Annex-D** – Supports LMI as specified by ANSI T1.617, Annex D.

Table 4-13. Interface Frame Relay Options (2 of 3)

Traffic Policing
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether or not CIR (Committed Information Rate) and EIR (Excess Information Rate) will be enforced by the unit on frames being sent on network frame relay links. **Enable** – CIR and EIR are enforced. ■ Frames that exceed CIR will be marked Discard Eligible (DE). These frames are counted in the **`Above CIR but within EIR`** category until this category is full. Once full, additional frames are counted as being in the **`Within CIR`** category. ■ Frames in excess of EIR will be discarded. ■ For CSU/DSUs only, DE frames received from the external router are credited as frames transmitted above CIR. They are credited as frames transmitted between CIR and EIR until that count reaches its limit, at which point they are counted as frames transmitted above EIR. **Disable** – CIR and EIR are not enforced.
LMI Parameters
Possible Settings: **System**, **Custom** Default Setting: **System**
Allows you to use the system LMI options, or to set specific LMI options for this interface. **System** – Use system LMI options (see Table 4-1, System Frame Relay and LMI Options). **Custom** – Use the following options in this table to configure LMI parameters.
Frame Relay DS0s Base Rate
Possible Settings: **Nx64**, **Nx56** Default Setting: **Nx64**
Selects the base rate for the DS0s allocated to frame relay on the network interface. *Display Conditions* – This option only appears on the network interface of the FrameSaver SLV 9128, not the 9128-II. **Nx64** – The base rate is 64 Kbps. **Nx56** – The base rate is 56 Kbps.
LMI Error Event (N2)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **3**
Configures the LMI-defined N2 parameter, which sets the number of errors that can occur on the LMI link before an error is reported. Applies to both the user and network sides of a UNI. **1 – 10** – Specifies the maximum number of errors.

Table 4-13. Interface Frame Relay Options (3 of 3)

LMI Clearing Event (N3)
Possible Settings: **1, 2, 3, 4, 5, 6, 7, 8, 9, 10** Default Setting: **1**
Configures the LMI-defined N3 parameter, which sets the number of error-free messages that must be received before clearing an error event. Applies to both the user and network sides of a UNI. **1 – 10** – Specifies how many error-free messages it will take to clear the error event.
LMI Status Enquiry (N1)
Possible Settings: **1, 2, 3, 4, . . . 255** Default Setting: **6**
Configures the LMI-defined N1 parameter, which sets the number of status enquiry polling cycles that the user side of the LMI initiates before a full status enquiry is initiated. Applies to the user side of a UNI only. **1 – 255** – Specifies the number of status enquiry polling cycles that can be initiated before a full status enquiry is initiated.
LMI Heartbeat (T1)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **10**
Configures the LMI-defined T1 parameter, which sets the number of seconds between the initiation of status enquiry messages on the user side of the LMI. Applies to the user side of a UNI only. **5 – 30** – Specifies the number of seconds between the initiation of status enquiry messages in increments of 5.
LMI Inbound Heartbeat (T2)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **15**
Configures the LMI-defined T2 parameter, which sets the number of seconds between the receipt of status enquiry messages on the network side of the LMI. Applies to the network side of a UNI only. **5 – 30** – Specifies the number of seconds between the receipt of status enquiry messages in increments of 5.
LMI N4 Measurement Period (T3)
Possible Settings: **5, 10, 15, 20, 25, 30** Default Setting: **20**
Configures the LMI-defined T3 parameter, which is the time interval (in seconds) that the network side of the LMI uses to measure the maximum number of status enquiry messages that have been received (N4) from the user side. **5 – 30** – Specifies the interval of time in increments of 5.

Manually Configuring DLCI Records

The Auto-Configuration feature automatically configures DLCI Records and their PVC Connections. DLCI Records can also be created manually (see Table 4-14, DLCI Record Options).

Main Menu → Configuration → [Network/Data Port/ISDN/Virtual Router Ports] → DLCI Records

Available paths to DLCI Records Options depend on the FrameSaver model:

- Data Port is available only on CSU/DSUs
- ISDN is available only when the FrameSaver unit has an ISDN DBM installed
- Virtual Router Ports is available only on the FrameSaver SLV Router

Typically, DLCI Records only need to be configured when building Management PVCs between the NOC and the central site unit; the unit automatically configures non-management DLCI Records and PVC Connections.

Table 4-14. DLCI Record Options (1 of 4)

DLCI Number
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the number for the DLCI in the DLCI record. The parameter determines which DLCI record is used for transferring data on a particular frame relay interface. DLCI numbers range from 0 to 1023. However, the numbers 0 – 15 and 1008 – 1023 are reserved. Entry of an invalid number results in the error message **`Value Out of Range (16–1007)`**. If the DLCI number is part of a connection, this field is read-only. NOTES: – If a DLCI number is not entered, the DLCI record is not created. – The DLCI number entered must be unique for the interface. – Changing settings for this configuration option causes the FrameSaver unit to abort any active frame relay tests. **16 – 1007** – Specifies the DLCI number (inclusive).

Table 4-14. DLCI Record Options (2 of 4)

DLCI Type
Possible Settings: **Standard, Multiplexed, IP Enabled** Default Setting: *For user data port DLCIs:* **Standard** *For network interface DLCIs:* **Multiplexed**
Specifies whether the DLCI is standard or multiplexed. This field is read-only when the selected DLCI is used in a PVC or Management link connection and the DLCI Type is Standard. *Display Conditions* – This option does not appear for a user data port or a virtual router port, and it cannot be changed if the DLCI is specified as the TS Access Management Link. **Standard** – Supports standard DLCIs as specified by the Frame Relay Standards. Use this setting when a non-FrameSaver unit is at the other end. **Multiplexed** – Enables multiplexing of multiple connections into a single DLCI. Allows a single PVC through the frame relay network to carry multiple DLCIs as long as these connections are between the same two endpoints (proprietary). Do not select Multiplexed unless there are FrameSaver units at both ends of the connection. **IP Enabled** – Enables connection to one or more endpoints through a Layer 3 network. A Payload Management PVC is created as well as the IP Enabled DLCI.
CIR (bps)
Possible Settings: **0 – 1536000** Default Setting: **0**
Determines the data rate for the DLCI that the network commits to accept and carry without discarding frames; the CIR in bits per second. Entry of an invalid rate causes the error message **`Value Out of Range (0 –`** *x***`)`**, where *x* = the maximum line rate available on the port. **0 – 1536000** – Specifies the network-committed data rate.
Tc
Possible Settings: **1 – 65535** Default Setting: Read Only
Displays the DLCI's calculated value of its committed rate measurement interval (Tc) in milliseconds. This value is calculated based upon the settings for the Committed Burst Size Bc (Bits) and CIR (bps) options.
Committed Burst Size Bc (Bits)
Possible Settings: **CIR, Other** Default Setting: **CIR**
Specifies whether the DLCI's committed burst size will follow the CIR, or whether it will be entered independently. This value is the maximum amount of data that the service provider has agreed to accept during the committed rate measurement interval (Tc). **CIR** – Uses the value in the CIR (bps) option as the committed burst size (Bc). The Bc and excess burst size (Be) options are updated when a CIR update is received from the network switch. **Other** – Allows you to specify the committed burst size for the DLCI. When Other is selected, the Bc and Be values must be manually entered and maintained, as well.

Table 4-14. DLCI Record Options (3 of 4)

Bc
Possible Settings: **0 – 1536000** Default Setting: **0**
Allows you to display or change the DLCI’s committed burst size. *Display Conditions* – This option only appears when Committed Burst Size is set to Other. **0 – 1536000** – Specifies the DLCI’s committed burst size.
Excess Burst Size (Bits)
Specifies the maximum amount of data in bits that the network may accept beyond the CIR without discarding frames.
Be
Possible Settings: **0 – 1536000** Default Setting: **1536000**
Allows you to display or change the DLCI’s excess burst size. **0 – 1536000** – Specifies the DLCI’s excess burst size.
DLCI Priority
Possible Settings: **Low, Medium, High** Default Setting: **High**
Specifies the relative priority for data received on the DLCI from an attached device (also known as *quality of service*). All data on Port 1 is cut-through, as long as there is no higher-priority data queued from another user port. The DLCI priority set for an interface applies to data coming into that interface. For example, the priority set for DLCIs on Port 1 applies to data coming into Port 1 from the attached equipment (such as a router). NOTE: For units with multiple user data ports, since pipelining occurs on Port-1, it is recommended that higher priority data be connected to Port-1 . *Display Conditions* – This option is not available for the network interface or, if the model has ISDN backup capability, an ISDN DBM interface. **Low** – Data configured for the DLCI has low priority. **Medium** – Data configured for the DLCI has medium priority. **High** – Data configured for the DLCI has high priority.
Outbound Management Priority
Possible Settings: **Low, Medium, High** Default Setting: **Medium**
Specifies the relative priority for management traffic sent on management PVCs on this DLCI to the network. *Display Conditions* – This option is not available on a user data port or a virtual router port. **Low** – Management data configured for the DLCI has low priority. **Medium** – Management data configured for the DLCI has medium priority. **High** – Management data configured for the DLCI has high priority.

Table 4-14. DLCI Record Options (4 of 4)

Backup Group
Possible Settings: **A, B, C, . . . Z, None** Default Setting: **None**
Assigns DLCIs to a backup group so backup does not take place unless all DLCIs in the group are no longer operational or latency has been exceeded. Backup is terminated when one DLCI in the group is operational again. This feature reduces backup charges when redundant PVCs have been configured. *Display Conditions* – This option is not available on a user data port, a virtual router port, or an ISDN DBM interface. **A – Z** – Specifies the designation for this group of DLCIs. Only DLCIs in a PVC will be considered part of a Backup Group. **None** – No Backup Groups have been set up.

Configuring PVC Connections

The Auto-Configuration feature automatically configures PVC Connections and their DLCI Records. PVC Connections can also be created manually (see Table 4-15, PVC Connection Options).

Main Menu→Configuration→PVC Connections

From this screen, you can go directly to the Management PVC screen by selecting the MgmtPVCs function key for easy movement between screens.

Quick removal of unused DLCIs (and ISDN Link Profiles, except for HQ_Site, if the model has an ISDN DBM installed) included in an existing PVC Connection is also available when the Delete function key is selected and you respond Yes to the **Remove otherwise unused components associated with the deleted PVC?** prompt.

Table 4-15. PVC Connection Options (1 of 4)

Source Link
Possible Settings: **Port-*n*, *ISDN Link Name*, Net1-FR1, Rtr-S0** Default Setting: Initially blank; no default.
Specifies the frame relay interface that starts a PVC connection; the **from** end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined that are not part of a PVC connection or management link. For example, if Port-1 has no DLCIs defined, Port-1 would not appear as a valid setting. **Net1-FR1** – Specifies that the network interface be used in the connection. ***ISDN Link Name*** – For units with ISDN backup capability, specifies the ISDN link of the DBM as the source link. This can be any nonnull link name configured on an ISDN frame relay link. **Port-*n*** – For CSU/DSUs, specifies that the frame relay link on the user data port be used in the connection. **Rtr-S0** – For the FrameSaver SLV 9126-II Router, specifies that the frame relay link on the virtual router port be used in the connection. **Clear All** – Clears all Link and DLCI settings, and suppresses EDLCIs.
Source DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the source DLCI for a frame relay interface. The DLCI must be defined and cannot be part of a PVC connection or management link. For multiplexed DLCIs, at least one EDLCI must be unconnected for the DLCI to be a valid selection. NOTE: Source DLCI has no value if Source Link contains no value. **16 – 1007** – Specifies the DLCI number.

Table 4-15. PVC Connection Options (2 of 4)

Source EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the source Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection. *Display Conditions* – This option only appears when Source DLCI contains a multiplexed DLCI record number. **0 – 62** – Specifies the EDLCI number.
Primary Destination Link
Possible Settings: **Net1-FR1, *ISDN Link Name*, Rtr-S0** Default Setting: Initially blank; no default.
Specifies the frame relay interface used as the primary destination link; the **to** end of a from-to link. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined which are not part of a PVC connection or management link. For example, if the network interface has no DLCIs defined, Net1-FR1 would not appear as a valid setting. **Net1-FR1** – Specifies the Network interface as the destination link. ***ISDN Link Name*** – For units with ISDN backup capability, specifies the ISDN link of the DBM as the destination of the connection. This can be any nonnull link name configured on an ISDN frame relay link. **Rtr-S0** – For the FrameSaver SLV 9126-II Router, specifies the virtual router port as the destination link.
Primary Destination DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the primary destination DLCI for a frame relay interface. The DLCI must be defined and cannot be part of a PVC connection or management link. For multiplexed DLCIs, at least one EDLCI must be unconnected for the DLCI to be a valid selection. NOTES: – Primary Destination DLCI has no value if Primary Destination Link contains no value. – When an ISDN DBM is installed and the DLCI assigned to the PVC is in a Backup Group (see Table 4-14, DLCI Record Options), the letter designation assigned to the group of DLCIs appears next to the primary destination DLCI number on the Management PVCs Options screen. **16 – 1007** – Specifies the DLCI number.

Table 4-15. PVC Connection Options (3 of 4)

Primary Destination EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the primary destination Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a connection. *Display Conditions* – This option only appears when the Primary Destination DLCI contains a multiplexed DLCI record number. For a DLCI that is: – IP Enabled, **IP** appears in this field – Payload Managed (but not IP Enabled), **PM** appears in this field **0 – 62** – Specifies the EDLCI number.
Alternate Destination Link
Possible Settings: **Net1-FR1, *ISDN Link Name*** Default Setting: Initially blank; no default.
Specifies the frame relay interface used as the alternate destination link; the *to* end of a from-to link that is used for backup when the primary destination link or DLCI is out of service. The only valid settings for this configuration option are frame relay interfaces that have at least one DLCI or EDLCI defined which are not part of a PVC connection or management link. For example, if *ISDN Link Name* has no DLCIs defined, the ISDN link name would not appear as a valid setting. **Net1-FR1** – Specifies the Network interface as the destination link. ***ISDN Link Name*** – Specifies the ISDN link of the DBM as the destination of the connection. This can be any non-null link name configured on an ISDN frame relay link on an installed DBM. **Clear Alternate** – Clears the Alternate Destination Link and Alternate Destination DLCI settings, and suppresses Alternate Destination EDLCI.
Alternate Destination DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the alternate destination Data Link Connection Identifier (DLCI) for a frame relay interface used for backup. The DLCI must be defined and cannot be part of a PVC connection or management link. For multiplexed DLCIs, at least one EDLCI must be unconnected for the DLCI to be a valid selection. *Display Conditions* – This option does not appear when the Alternate Destination Link contains no value. **16 – 1007** – Specifies the DLCI number.

Table 4-15. PVC Connection Options (4 of 4)

Alternate Destination EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the alternate destination Embedded Data Link Connection Identifier (EDLCI) for a frame relay interface when a multiplexed DLCI record is selected as one end of a backup connection. *Display Conditions* – This option only appears when the Alternate Destination DLCI contains a multiplexed DLCI record number. **0 – 62** – Specifies the EDLCI number.

Configuring the IP Path List

Select IP Path List (Static) from the Configuration Edit/Display menu to display or change the list of static path IP addresses explicitly defined in the unit.

Main Menu→Configuration→IP Path List (Static)

The IP Path List (Static) screen appears, showing any existing static paths. Paths discovered as SLV packets are received from other FrameSaver units are not shown. To view the entire current IP Path List, use the IP Path Connection Status screen. See *IP Path Connection Status* in Chapter 7, *Operation and Maintenance*.

▶ Procedure

To add a static path:

1. Select New. The following prompt appears:

   ```
   Enter IP Address (press ESC to abort): ___.___.___.___ FWD: No_
   ```

2. Enter the IP address of a static path and select a forwarding option of No or Yes using the spacebar.

3. Press enter. Select Save.

Table 4-16. IP Path List

IP Address
Possible Settings: **000.000.000.001 – 126.255.255.255, 128.000.000.000 – 223.255.255.255** Default Setting: Initially blank; no default.
Specifies the address of a FrameSaver or other device at the other end of a path. **000.000.000.001 – 126.255.255.255, 128.000.000.000 – 223.255.255.255** – Specifies the address of a device.
FWD
Possible Settings: **No, Yes** Default Setting: **No**
Determines whether this path list item is sent to all other addresses in the list that represent FrameSaver devices. **No** – The IP address associated with this path list item is not distributed. **Yes** – The IP address associated with this path list entry is distributed to devices in the list.

Setting Up Management and Communication Options

Management and Communications options are explained in the following sections:

- *Configuring Node IP Information*
- *Configuring Management PVCs*
- *Configuring General SNMP Management*
- *Configuring Telnet and/or FTP Session Support*
- *Configuring SNMP NMS Security*s
- *Configuring SNMP Traps and Trap Dial-Out*
- *Configuring Ethernet Management*
- *Configuring the Communication Port*
- *Configuring the Modem Port*
- *Configuring the Criteria for Automatic Backup*

Configuring Node IP Information

Select Node IP to display, add, or change the information necessary to support general IP communications for the node (see Table 4-17, Node IP Options). When deploying units to remote sites, minimally configure the Node IP Address and Subnet Mask.

Main Menu→Configuration→Management and Communication→Node IP

This set of configuration options includes a Troubleshooting (TS) Management Access Link feature to help service providers isolate device problems within their networks. This feature allows Telnet or FTP access to the unit on this link. Troubleshooting over this link is essentially transparent to customer operations. No alarms or SNMP traps are generated to create nuisance alarms for the customer.

TS_Access_Management_Link is initially disabled in most models, but the link can be enabled at any time. Any valid network Management PVC created on a standard DLCI can be used. When enabled, a troubleshooting link can be accessed any time the service provider requests access. An assigned security level can also control access.

When a DLCI has been defined as the troubleshooting management link, the link is identified in the status field at the bottom of the Management PVC Entry screen with the **`Note: This PVC has been designated as the TS Access Management Link`** message.

NOTE:

The unit may come from the factory with a TS Management PVC already set up (e.g., 980).

Table 4-17. Node IP Options (1 of 3)

Node IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the node. Since an IP address is not bound to a particular port, it can be used for remote access via a management PVC. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the node, which can be viewed or edited. **Clear** – Fills the node IP address with zeros.
Node Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the node. Since the subnet mask is not bound to a particular port, it can be used for remote access via a management PVC. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the node, which can be viewed or edited. **Clear** – Fills the node subnet mask with zeros. When the node's subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Table 4-17. Node IP Options (2 of 3)

Default IP Destination

Possible Settings: **None, Modem, COM, Ethernet, *PVCname***
Default Setting: **None**

Specifies an IP destination to route data that does not have a specifically defined route.

Examples:

- If the default IP network is connected to the communications port, select COM.
- If the default IP network is connected to a far-end device over the management PVC named London for the remote device located in the London office, select the PVC name London (as defined by the Name configuration option, Table 4-18, Management PVC Options).

  NOTE: If the link to the IP destination selected as the default route becomes disabled or down, the unrouteable data will be discarded. Make sure that the link selected is operational, and if that link goes down, change the default destination.

  CAUTION: Use care when configuring a default route to an interface that has a subnet route configured at a remote end where the NMS, router, LAN adapter, terminal server, etc. is connected. Communicating with an unknown IP address on the subnet will cause temporary routing loops, which will last 16 iterations times the retry count.

None – No default network destination is specified. Unrouteable data will be discarded. This is the recommended setting.

Modem – Specifies that the default destination is connected to the modem port. Only appears when the modem port Use option is set to Net Link.

COM – Specifies that the default destination is connected to the COM port. Only appears when Port Use is set to Net Link (see Table 4-24, Communication Port Options).

Ethernet – For the FrameSaver SLV 9126-II or 9128-II, specifies that the default destination is connected to the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled. When selected, the Default Gateway Address must also be configured (see Table 4-23, Ethernet Management Options).

PVCname – Specifies a name for the management PVC. Only appears when a management PVC name is defined for the node. For example, when the network is connected to a remote device located in the London office, London can be specified as the PVC name, which is the link between the local FrameSaver unit and the one located in London. London would appear as one of the available selections.

TS Access Management Link

Available Settings: **None, *PVCname***
Default Setting: **None**

Specifies a troubleshooting management link for the special needs of network service providers.

If the setting is changed from the management PVC name to None, the **Delete the Management PVC *PVCname* and the associated DLCI Record?** prompt appears. If you select:

- No – The link designation is removed and the option is set to None.
- Yes – The link designation is removed and the option is set to None, and the link and its DLCI will be deleted.

None – Disables or does not specify a TS Access Management Link.

PVCname – Specifies the name of the TS Management PVC.

Display Conditions – This selection only appears when a dedicated management PVC has been defined on the network frame relay link as a DLCI with DLCI Type set to Standard.

Table 4-17.   Node IP Options (3 of 3)

TS Management Link Access Level
Available Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest access level allowed when accessing the unit via a Telnet or FTP session when the service provider is using the TS Access Management Link. *Display Conditions* – This option only appears when: ■ Service Type on the Easy Install screen is set to Frame Relay. ■ TS Access Management Link is set to a PVC name. NOTES: – Telnet and FTP sessions on this link *are not* affected by the access level set by the Session Access Level, Login Required, or FTP Login Required option settings (see Table 4-20, Telnet and FTP Session Options). – Telnet and FTP sessions on this link *are* affected by the Telnet Session, Inactivity Timeout, Disconnect Time and FTP Session option settings. **Level-1** – Allows Telnet or FTP access by network service providers with the capability to view unit information, change configuration options, and run tests. This is the highest access level allowed. Use this setting when downloading files. **Level-2** – Allows Telnet or FTP access by network service providers with the capability to view unit information and run tests only; they cannot change configuration options. **Level-3** – Allows Telnet access by network service providers with the capability to view unit information only; they cannot change configuration options or run tests.
TS Management SNMP Validation
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether validation of community strings and IP addresses is performed for this management link. *Display Conditions* – This option only appears when: ■ Service Type on the Easy Install screen is set to Frame Relay. ■ TS Access Management Link is set to a PVC name. **Enable** – Validation of community strings and IP addresses is performed on SNMP traffic. **Disable** – No validation of community strings and IP addresses is performed.

Configuring Management PVCs

Select Management PVCs to define inband management links by adding or changing Management PVCs (see Table 4-18, Management PVC Options). First, DLCI records must have been configured for the interface where the Management PVC will reside. See *Manually Configuring DLCI Records* on page 4-64 for additional information.

Main Menu→Configuration→Management and Communication→ Management PVCs

Select New or Modify to add or change Management PVCs.

- When you select New, the configuration option field is blank.
- When you select Modify, the values displayed for all fields are based on the PVC ID number that you specified.

These options do not apply when the Management PVC is designated as a TS Management Link (see *Configuring Node IP Information* on page 4-74 for additional information).

From this screen, you can go directly to the PVC Connections screen by selecting the PVCConn function key for easy movement between screens.

Select the Delete function key, a Management PVC ID#, and respond Yes to the **`Remove otherwise unused components associated with the deleted PVC?`** prompt for quick removal of unused DLCIs. If the Management PVC selected is defined as a trap Initial Route Destination, a Default IP Destination, or a TS Access Management Link, an ... **`Are You Sure?`** prompt is displayed to warn you.

A payload management circuit is identified by **`PM`** in the EDLCI field of the Management PVCs Options screen. If a payload management management circuit is deleted, the associated PVC remains standard, even if was a multiplexed PVC (automatically converted to standard) when it the management circuit was created.

If an existing PVC with an associated payload managed management circuit is deleted, then the payload management circuit is also deleted.

Table 4-18. Management PVC Options (1 of 6)

Name
Possible Settings: ***ASCII Text Entry*** Default Setting: Initially blank; no default.
Specifies a unique name for the management PVC as referenced on screens (e.g., Tampa for Tampa, Florida). ***ASCII Text Entry*** – Enter a unique name for the management PVC (maximum length 8 characters).

Table 4-18. Management PVC Options (2 of 6)

Payload Managed
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether the PVC is payload managed. *Display Conditions* – This is a read-only field set to Enabled if the PVC is IP Enabled. **Enable** – The network PVC created will be monitored for the presence of IP frames containing the IP address specified in the Intf IP Address field. When such a frame is identified, it is extracted from the data stream and sent to the management stack. **Disable** – A normal management PVC is created using the specified DLCI or EDLCI.
Intf IP Address
Possible Settings: **Node-IP-Address, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-IP-Address**
Specifies the IP address needed to access the unit via this management PVC, providing connectivity to an external IP network through the frame relay network. **Node-IP-Address** – Uses the IP address contained in the Node IP Address (see Table 4-17, Node IP Options). **Special** (001.000.000.000 – 223.255.255.255) – Allows you to display/edit an IP address for the unit's management PVC when the IP address for this interface is different from the node's IP address.
Intf Subnet Mask
Possible Settings: **Node-Subnet-Mask, Calculate, Special** (*nnn.nnn.nnn.nnn*) Default Setting: **Node-Subnet-Mask**
Specifies the subnet mask needed to access the unit when the management PVC is providing connectivity to an external IP network (through frame relay) that requires a specific subnet mask for the interface. **Node-Subnet-Mask** – Uses the *Interface* IP Subnet contained in the Node-Subnet Mask configuration option (see Table 4-17, Node IP Options). **Calculate** – Calculates the subnet mask created by the IP protocol based on the class of the IP address (Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000). Cannot be displayed or edited. **Special** (000.000.000.000 – 255.255.255.255) – Allows you to edit/display the subnet mask for the management PVC when the subnet mask is different for this interface. A text field displays where you can enter the subnet mask for this unit's management PVC.
Set DE
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether frames (packets) sent on a management PVC have the Discard Eligible (DE) bit set. This bit is used by the network to prioritize which frames to discard first during periods of network congestion. This allows management traffic to be viewed as lower priority than customer data. **Enable** – Sets the DE bit to one on all frames sent on the management PVC. **Disable** – Sets the DE bit to zero on all frames sent on the management PVC. This is the recommended setting, particularly for NSPs providing a managed network service.

Table 4-18. Management PVC Options (3 of 6)

Primary Link
Possible Settings: **Net1-FR1, Port-*n*, Rtr-S0, *ISDN Link Name*, Clear** Default Setting: Initially blank; no default.
Specifies the frame relay interface to use for this management PVC. The interface selected must have at least one DLCI (or DLCI with EDLCI) defined, which is not part of a PVC connection or already assigned as a management PVC. *Display Conditions* – The Port-1 setting does not appear if the PVC is IP Enabled or Payload Managed is enabled. **Net1-FR1** – Specifies the network interface as the source link for the connection. **Port-*n*** – Specifies the frame relay link on the user data port as the destination link for the connection. **Rtr-S0 –** For the FrameSaver SLV 9126-II Router, specifies that the virtual router port be used in the connection. ***ISDN Link Name*** – For units with ISDN backup capability, specifies the ISDN link on the DBM to be used in the connection. This can be any nonnull link name configured on an ISDN frame relay link on an installed DBM. **Clear** – Clears the link and the DLCI field, and suppresses the EDLCI field if the DLCI was multiplexed.
Primary DLCI
Possible Settings: **16 – 1007** Default Setting: Initially blank; no default.
Specifies the DLCI number used for the management PVC after the frame relay interface is selected. The DLCI must be defined for the link (i.e., has a DLCI record), and it must not be part of a PVC connection or already assigned as a management PVC. For multiplexed DLCIs, at least one EDLCI must be unconfigured for the DLCI. NOTES: – DLCI cannot be entered if the Link field is blank. – Clearing the Link also clears the DLCI. – When an ISDN DBM is installed and the DLCI assigned to the PVC is in a Backup Group (see Table 4-14, DLCI Record Options), the letter designation assigned to the group of DLCIs appears next to the primary destination DLCI number on the Management PVCs Options screen. **16 – 1007** – Specifies the DLCI number (inclusive).

Table 4-18. Management PVC Options (4 of 6)

Primary EDLCI
Possible Settings: **0 – 62** Default Setting: Initially blank; no default.
Specifies the EDLCI number used for a management PVC when a multiplexed DLCI is selected. EDLCIs identify individual connections within multiplexed DLCIs that are unique to those DLCIs. Use a unique EDLCI to identify an individual connection within a multiplexed DLCI. Use 0 to identify the primary EDLCI. Use 1 – 62 to identify secondary EDLCIs. Use the primary EDLCI for customer data, which has a higher utilization rate than management data, with slightly less line overhead. *Display Conditions* – This option does not appear if the DLCI field does not reference a multiplexed DLCI, if the PVC is IP Enabled, or if Payload Managed is enabled. NOTE: Clearing the DLCI or changing it to a standard DLCI suppresses EDLCI field. **0 – 62** – Specifies the EDLCI number (inclusive).
Primary Link RIP
Possible Settings: **None, Proprietary, Standard_out** Default Setting: *For multiplexed DLCIs:* **Proprietary** *For nonmultiplexed DLCIs:* **Standard_out**
Specifies which Routing Information Protocol (RIP) is used to enable routing of management between FrameSaver units and attached equipment. *Display Conditions* – This option does not appear if the PVC is IP Enabled or Payload Managed is enabled. **None** – Does not use a routing protocol. **Proprietary** – Uses a proprietary variant of RIP version 1 to communicate routing information between FrameSaver units. A FrameSaver unit must be on the other end of the link. This is the factory default for management PVCs configured on multiplexed DLCIs (see Table 4-14, DLCI Record Options). **Standard_out** – The device will send standard RIP messages to communicate routing information only about FrameSaver SLV and FLEX devices in the network. This is the factory default for management PVCs configured on standard DLCIs. NOTE: The router must be configured to receive RIP on the port connected to the FrameSaver unit for the management interface (e.g., Cisco: **`config-t, router RIP, int serialx, IP RIP Receive version 1, ctl-z WR`**). See *Using RIP with FrameSaver SLV CSU/DSUs* on page 4-4.

Table 4-18. Management PVC Options (5 of 6)

Alternate Link

Possible Settings: **Net1-FR1, Port-*n*, *ISDN Link Name*, Clear**
Default Setting: Initially blank; no default.

Specifies the frame relay interface to use for this management PVC as the alternate link. The interface selected must have at least one DLCI (or DLCI with EDLCI) defined, which is not part of a PVC connection or already assigned as a management PVC.

> *Display Conditions* – This option does not appear unless ISDN backup is available, and does not appear if Payload Managed is enabled.

Net1-FR1 – Specifies the Network interface as the frame relay link.

Port-*n* – Specifies the frame relay link on the user data port as the alternate destination link for the connection.

ISDN Link Name – For units with ISDN backup capability, specifies the ISDN link of the DBM to be used in the connection. This can be any nonnull link name configured on an ISDN frame relay link on an installed DBM.

Clear – Clears the link and the DLCI field, and suppresses the EDLCI field if the DLCI was multiplexed.

Alternate DLCI

Possible Settings: **16 – 1007**
Default Setting: Initially blank; no default.

Specifies the alternate DLCI number to be used for the management PVC after the frame relay interface is selected.

The DLCI must be defined for the link (i.e., has a DLCI record), and it must not be part of a PVC connection or already assigned as a management PVC. For multiplexed DLCIs, at least one EDLCI must be unconfigured for the DLCI.

> *Display Conditions* – This option does not appear if Payload Managed is enabled. The DLCI cannot be entered if the Link field is blank.
>
> NOTE: Clearing Link also clears the DLCI.

16 – 1007 – Specifies the DLCI number (inclusive).

Alternate EDLCI

Possible Settings: **0 – 62**
Default Setting: Initially blank; no default.

Specifies the alternate EDLCI number used for a management PVC when a multiplexed DLCI is selected for the frame relay link. EDLCIs identify individual connections within multiplexed DLCIs that are unique to those DLCIs.

Use a unique EDLCI to identify an individual connection within a multiplexed DLCI. Use 0 to identify the primary EDLCI. Use 1 – 62 to identify secondary EDLCIs. Use the primary EDLCI for customer data, which has a higher utilization rate than management data, with slightly less line overhead.

> *Display Conditions* – This option does not appear unless ISDN backup is available and the DLCI field does not reference a multiplexed DLCI. This option does not appear if Payload Managed is enabled.
>
> NOTE: Clearing the DLCI or changing it to a standard DLCI suppresses the EDLCI field.

0 – 62 – Specifies the EDLCI number (inclusive).

Table 4-18. Management PVC Options (6 of 6)

Encapsulation
Possible Settings: **Routed** Default Setting: **Routed**
This read-only field specifies that the IP encapsulation used is RFC 1490/RFC 2427 routed Network Level Protocol IDentifier (NLPID) encapsulation, and not SubNetwork Access Protocol (SNAP) encapsulation. *Display Conditions* – This option appears only if the PVC is IP Enabled or Payload Managed is enabled. **Routed** – IP encapsulation is routed NLPID.

Configuring General SNMP Management

Select General SNMP Management to add, change, or delete the information needed to allow the FrameSaver unit to be managed as an SNMP agent by the NMS supporting the SNMP protocols (see Table 4-19, General SNMP Management Options).

> *Main Menu→Configuration→Management and Communication→ General SNMP Management*

You must have Level-1 access to display or configure these options.

Table 4-19. General SNMP Management Options (1 of 2)

SNMP Management
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the FrameSaver unit can be managed as an SNMP agent by an SNMP-compatible NMS. **Enable** – Can be managed as an SNMP agent. **Disable** – Cannot be managed as an SNMP agent. The FrameSaver unit will not respond to SNMP messages nor send SNMP traps.
Community Name 1
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Public** in ASCII text field
Specifies the first of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 1 (maximum 255 characters). **Clear** – Clears Community Name 1.
Name 1 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read/Write**
Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 1. **Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP **get** and **set** commands).
Community Name 2
Possible Settings: ***ASCII text entry*, Clear** Default Setting: **Clear**
Specifies the second of two names that are allowed to access the objects in the FrameSaver unit's MIB. The community name must be supplied by an external SNMP manager whenever the manager tries to access an object in the MIB. ***ASCII text entry*** – Adds to or changes Community Name 2 (maximum 255 characters). **Clear** – Clears Community Name 2.

Table 4-19. General SNMP Management Options (2 of 2)

Name 2 Access
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of access allowed to the objects in the MIB. This is the type of access allowed for external SNMP managers accessing MIB objects using Community Name 2. **Read** – Allows read-only access (SNMP Get command). This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP **get** and **set** commands).

Configuring Telnet and/or FTP Session Support

Telnet and FTP options control whether a Telnet or FTP (File Transport Protocol) session is allowed through an interconnected IP network and the access security applicable to the session. Two Telnet sessions can be active at a time (see Table 4-20, Telnet and FTP Session Options).

Main Menu→Configuration→Management and Communication→
Telnet and FTP Session

When a TS Access Management Link has been set up and activated, the following options have no effect upon the PVC:

- Telnet Login Required
- Session Access Level
- FTP Login Required

Table 4-20. Telnet and FTP Session Options (1 of 2)

Telnet Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether the FrameSaver unit will respond to a session request from a Telnet client on an interconnected IP network. **Enable** – Allows Telnet sessions between the FrameSaver unit and Telnet client. **Disable** – Does not allow Telnet sessions.
Telnet Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a user ID and password (referred to as the login) are required to access the menu-driven user interface via a Telnet session. If required, the login used is the same login used for an menu-driven user interface session. This option does not affect the TS Access Management Link. **Enable** – Requires a login to access a Telnet session. **Disable** – Does not require a login.
Session Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the highest security level allowed when accessing the menu-driven user interface via a Telnet session. If a login is required for the session, the effective access level is also determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. This option does not affect the TS Access Management Link. NOTE: The effective access level is always the lowest one assigned to either the session or the user. For example, if the assigned Session Access Level is Level-2, but the User Access Level is Level-3, then only level-3 access is allowed for the session. **Level-1** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information, change configuration options, and run tests. This is the highest access level allowed. CAUTION: Before changing the session access level to Level-2 or 3, make sure that the COM port's Port Access Level is set to Level-1 and that at least one Login ID is set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. A reset is required if the Communication Port's Port Use option is set to Net Link (see Table 4-5, General System Options). **Level-2** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information and run tests only; they cannot change configuration options. **Level-3** – Allows Telnet access by users with Login ID access levels of 1, 2, and 3, with the capability to view system information only; they cannot change configuration options or run tests.

Table 4-20. Telnet and FTP Session Options (2 of 2)

Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a Telnet session is disconnected after a specified period of keyboard inactivity. **Enable** – Terminates the session after the Disconnect Time expires. **Disable** – Does not terminate Telnet session during inactivity.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Sets the amount of keyboard inactive time allowed before a user session is disconnected. *Display Conditions* – This option does not appear when Inactivity Timeout is disabled. **1 – 60** – Up to an hour can be set.
FTP Session
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the system responds as a server when an FTP (file transfer protocol) client on an interconnected IP network requests an FTP session. This option must be enabled when downloading files. **Enable** – Allows an FTP session between the system and an FTP client. **Disable** – Does not allow FTP sessions.
FTP Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether a login ID and password are required for an FTP session. If required, the login used is the same login used for a menu-driven user interface session. This option does not affect the TS Access Management Link. **Enable** – User is prompted for a login ID and password. **Disable** – No login is required for an FTP session.
FTP Max Transfer Rate (Kbps)
Possible Settings: **1 – 1536** Default Setting: **1536**
Sets the maximum receive (or send) rate of file transfer to the system via management PVCs. This option allows new software and configuration files to be downloaded using selected bandwidth without interfering with normal operation. Using this option, new software and configuration files can be downloaded quickly using the default settings, or at a slower rate over an extended period of time by selecting a slower speed. Based upon TCP flow control, the FTP server in the system throttles bandwidth to match this setting. **1 – 1536** – Sets the download line speed from 1 kilobits per second to the maximum management speed.

Configuring SNMP NMS Security

Select SNMP NMS Security from the Management and Communication menu to display, add, or change SNMP security configuration options for the FrameSaver unit to set up trap managers (see Table 4-21, SNMP NMS Security Options).

Main Menu→Configuration→Management and Communication→ SNMP NMS Security

A table is displayed consisting of the network management systems identified by IP address that are allowed to access the FrameSaver unit by SNMP.

Table 4-21. SNMP NMS Security Options (1 of 2)

NMS IP Validation
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Specifies whether security checks are performed on the IP address of SNMP management systems attempting to access the node. Only allows access when the sending manager's IP address is listed on the SNMP NMS Security Options screen. **Enable** – Performs security checks. **Disable** – Does not perform security checks.
Number of Managers
Possible Settings: **1 – 10** Default Setting: **1**
Specifies the number of SNMP management systems that are authorized to send SNMP messages to the FrameSaver unit. An IP address must be configured for each management system allowed to send messages. Configure IP addresses in the NMS *n* IP Address configuration option. **1 – 10** – Specifies the number of authorized SNMP managers.
NMS *n* IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Provides the IP address of an SNMP manager that is authorized to send SNMP messages to the unit. If an SNMP message is received from an unauthorized NMS and its IP address cannot be matched here, access is denied and an authenticationFailure trap is generated. If a match is found, the type of access (read-only or read/write) is determined by the corresponding Access Type. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds to or changes the NMS IP address. **Clear** – Fills the NMS IP address with zeros.

Table 4-21. SNMP NMS Security Options (2 of 2)

Access Type
Possible Settings: **Read, Read/Write** Default Setting: **Read**
Specifies the type of access allowed for an authorized NMS when IP address validation is performed. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **Read** – Allows read-only access (SNMP Get command) to the MIB objects. This includes all objects specified as either read-only or read/write in the MIB RFCs. **Read/Write** – Allows read and write access (SNMP Get and Set commands) to the MIB objects. However, access for all read-only objects is specified as read-only.

Configuring SNMP Traps and Trap Dial-Out

Select SNMP Traps from the Management and Communication menu to configure SNMP traps and dial-out when a trap is generated (see Table 4-22, SNMP Traps and Trap Dial-Out Options).

> *Main Menu→Configuration→Management and Communication→ SNMP Traps*

See Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*, for trap format standards and special trap features, including RMON-specific traps, and the default settings that will generate RMON-specific SNMP traps.

Table 4-22. SNMP Traps and Trap Dial-Out Options (1 of 6)

SNMP Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the FrameSaver unit sends trap messages to the currently configured SNMP trap manager(s). **Enable** – Sends trap messages. **Disable** – Does not send trap messages.
Number of Trap Managers
Possible Settings: **1 – 6** Default Setting: **1**
Specifies the number of SNMP management systems that will receive SNMP trap messages from the FrameSaver unit. An NMS IP Address must be configured in the NMS *n* IP Address configuration option for each trap manager to receive trap messages. **1 – 6** – Specifies the number of trap managers (inclusive).

Table 4-22. SNMP Traps and Trap Dial-Out Options (2 of 6)

NMS *n* IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address that identifies the SNMP manager(s) to receive SNMP traps. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **001.000.000.000 – 223.255.255.255** – Adds to or changes the IP address for the trap manager. **Clear** – Fills the NMS IP address with zeros.
Initial Route Destination
Possible Settings: **AutoRoute, Modem, COM, Ethernet, *PVCname*** Default Setting: **AutoRoute**
Specifies the initial route used to reach the specified Trap Manager. When proprietary RIP is active, only one unit in the network needs to specify an interface or management link as the initial destination. All other units can use the default setting. *Display Conditions* – This option appears for each trap manager specified in the Number of Trap Managers configuration option. **AutoRoute** – Uses proprietary RIP from other FrameSaver devices to learn the route for sending traps to the specified Trap Manager, or the Default IP Destination when no route is available in the routing table (see Table 4-17, Node IP Options). **Modem** – Uses the Modem port. This selection only appears if the Modem Port Use configuration option is set to Net Link (see Table 4-25, Modem Port Options). **COM** – Uses the COM port. This selection is only available when Port Use is set to Net Link (see Table 4-24, Communication Port Options). **Ethernet** – For the FrameSaver SLV 9126-II or 9128-II, uses the Ethernet port. Only appears when the Ethernet port's Interface Status option is enabled (see Table 4-23, Ethernet Management Options). ***PVCname*** – Uses the defined management *linkname* (the name given the Management PVC). This selection only appears when at least one Management PVC is defined for the node.
General Traps
Possible Settings: **Disable, Warm, AuthFail, Both** Default Setting: **Both**
Determines whether SNMP trap messages for warmStart and/or authenticationFailure events are sent to the currently configured trap manager(s). An authenticationFailure trap indicates that the unit is the addressee of an SNMP protocol message, or an incoming ISDN call is not properly authenticated. **Disable** – Does not send trap messages for these events. **Warm** – Sends trap messages for warmStart events only. **AuthFail** – Sends trap messages for authenticationFailure events only. **Both** – Sends trap messages for both warmStart and authenticationFailure events.

Table 4-22. SNMP Traps and Trap Dial-Out Options (3 of 6)

Enterprise Specific Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether trap messages for enterpriseSpecific events are sent to the currently configured trap manager(s). **Enable** – Sends trap messages for enterpriseSpecific events. **Disable** – Does not send trap messages for enterpriseSpecific events.
Link Traps
Possible Settings: **Disable, Up, Down, Both** Default Setting: **Both**
Determines whether SNMP linkDown or linkUp traps are sent to the currently configured trap manager(s). A linkDown trap indicates that the unit recognizes a failure in one of the interfaces. A linkUp trap indicates that the unit recognizes that one of its interfaces is active. Use the Link Traps Interface and the DLCI Traps on Interfaces configuration options to specify which interface will monitor linkUp and linkDown traps messages. **Disable** – Does not send linkDown or linkUp trap messages. **Up** – Sends trap messages for linkUp events only. **Down** – Sends trap messages for linkDown events only. **Both** – Sends trap messages for linkUp and linkDown events.
Link Traps Interfaces
Possible Settings: **Network, DSX-1, T1s, Ports, DBM, All** Default Setting: **All**
Specifies which interfaces will generate linkUp, linkDown, and enterpriseSpecific trap messages. These traps are not supported on the COM port or Modem port. **Network** – Generates these trap messages on the network interface only. **DSX-1** – For applicable T1 FrameSaver units, generates these trap messages on the DSX-1 interface only. **T1s** – For applicable T1 FrameSaver units, generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on both the T1 network and DSX-1 interfaces. **Ports** – Generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on a user data port only. **DBM** – For units with an ISDN DBM installed, generates these trap messages for linkUp, linkDown, and enterpriseSpecific events on the DBM only. **All** – Generates these trap messages for linkUp and enterpriseSpecific events on all interfaces, except for the COM port or modem port, that are applicable to the FrameSaver model.

Table 4-22. SNMP Traps and Trap Dial-Out Options (4 of 6)

DLCI Traps on Interfaces – Interface Selection Field
Possible Settings: **Network, Ports, DBM, All, None** Default Setting: **All**
Specifies which interfaces will generate linkUp and linkDown trap messages for individual DLCIs. These traps are only supported on the frame relay interfaces. **Network** – Generates these trap messages on DLCIs for the network interface only. **Ports** – Generates these trap messages for DLCIs on a user data port only. **DBM** – For units with an ISDN DBM installed, generates trap messages on DLCIs for the DBM only. **All** – Generates these trap messages on all frame relay interfaces. **None** – No DLCI trap messages are generated.
DLCI Traps on Interfaces – Filter Selection Field
Possible Settings: **Normal, Filter** Default Setting: **Normal**
Controls whether the traps on the interfaces specified in the DLCI Traps on Interfaces configuration option are sent regardless of their cause. **Normal** – Generates trap messages specified by DLCI Traps on Interfaces regardless of cause. **Filter** – Prevents traps from being generated for the interfaces specified by DLCI Traps on Interfaces if their cause is the loss of the interface connection or LMI.
RMON Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Specifies whether remote monitoring traps are sent to the currently configured trap manager(s). RMON traps are typically sent as a result of the Alarms and Events Groups of RMON1 when a selected variable’s configured threshold is exceeded. **Enable** – Sends trap messages when set thresholds are exceeded. **Disable** – Does not send trap messages when set thresholds are exceeded.
ISDN Dial Control Traps
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls whether dialCtlPeerCallSetup and dialCtlPeerCallInformation events send trap messages to the currently configured SNMP trap manager(s). Use this feature when peer-to-peer (nearest neighbor) calling is desired. *Display Conditions* – This option only appears when an ISDN DBM is installed. **Enable** – Sends trap messages. **Disable** – Does not send trap messages.

Table 4-22. SNMP Traps and Trap Dial-Out Options (5 of 6)

Trap Dial-Out
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls whether SNMP trap messages initiate a call automatically. If the call cannot be completed and the Call Retry option is set to Enable, the SNMP trap message is held (queued) until the call completes to either the Alarm or alternate directory. NOTE: When the modem port is configured as a network communication link, up to 10 SNMP trap messages are held at the port. **Enable** – Automatically calls the phone number contained in the Control menu's Modem Call Directories, Directory Number A (Alarm). **Disable** – Automatic calls will not be initiated. Traps sent to the modem are held until a dial-in connection is established.
Trap Disconnect
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether the internal modem disconnects after the SNMP trap message has been sent. This configuration option only applies to modem connections initiated as a result of sending the SNMP trap message. **Enable** – Disconnects the call after sending an SNMP trap message(s). **Disable** – Does not disconnect the call and holds the line until it is disconnected manually or by the remote modem. This allows the NMS to poll the FrameSaver unit for more information after receiving an SNMP trap.
Call Retry
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Controls whether an incomplete call (busy, no answer, etc.) is retried when an SNMP trap message is sent to the modem port. If an Alternate Dial-Out Directory is specified, the alarm directory's telephone number is called first. If the call cannot be completed, then the alternate directory's telephone number is called (see the Control menu's Modem Call Directories). **Enable** – Attempts to retry the call, up to one time per SNMP trap message, with a delay between the retry. The delay is specified by the Dial-Out Delay Time (Min) configuration option. **Disable** – Does not retry an incomplete call.
Dial-Out Delay TIme (Min)
Possible Settings: **1 – 10** Default Setting: **5**
Specifies the amount of time between call retries when an SNMP trap message is sent; the wait between call attempts (see the Call Retry option). **1 – 10** – Sets the number of minutes for the delay between call retry attempts.

Table 4-22. SNMP Traps and Trap Dial-Out Options (6 of 6)

Alternate Dial-Out Directory
Possible Settings: **None, 1 – 5** Default Setting: **None**
Specifies whether an incomplete call (busy, or no answer, etc.) resulting from an attempt to send an SNMP trap message is retried using an alternate telephone number. Up to 5 alternate call directories can be set up, but only one at a time can be used. When Call Retry is enabled, the alarm directory’s telephone number is called first. If the call cannot be completed after one additional try, then the specified alternate directory’s telephone number is called. **None** – Does not dial-out using one of the alternate directory telephone numbers. **1 – 5** – Specifies the call directory containing the telephone number to call if a call cannot be completed using the telephone number in the alarm directory (Directory Number A in the Control menu’s Modem Call Directories), inclusive.
Latency Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a Latency Threshold Alarm causes the generation of a Latency Threshold Exceeded Trap. **Enable** – Sends trap messages for Latency Threshold Alarm events. **Disable** – Does not send trap messages for Latency Threshold Alarm events.
IP SLV Availability Traps
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a Path Unavailability condition causes the generation of an IP SLV Availability Trap. **Enable** – Sends trap messages for Path Unavailability events. **Disable** – Does not send trap messages for Path Unavailability events.

Configuring Ethernet Management

For the FrameSaver SLV 9126-II or 9128-II, select Ethernet Management from the Management and Communication menu, or Ethernet Management Options Screen from the Easy Install screen, to configure the Ethernet port (see Table 4-23, Ethernet Management Options).

Main Menu→Configuration→Management and Communication→ Ethernet Management

Main Menu→Easy Install→Ethernet Management Options Screen

Table 4-23. Ethernet Management Options (1 of 2)

Interface Status
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the Ethernet port is being used and can be configured. **Enable** – The port is active. It can receive Version 2 or IEEE 802.3 MAC frames and transmit Version 2 MAC frames only. When the Ethernet port is enabled, the `Would you like to set the Node's IP Destination to Ethernet?` prompt is displayed. ■ If you select Yes, the Default IP Destination (see Table 4-17, Node IP Options) is automatically changed to Ethernet, so the Ethernet port's Default Gateway Address is used for packets that do not have a route. This is required when the NMS is on a different subnet than the unit. ■ If you select No, the COM port or a PVC will be used for packets without a route. **Disable** – The port is not active. When the port is disabled, the following will occur: ■ No alarms or traps configured for the port will be generated. ■ All port uses that refer to the Ethernet port, like the Default IP Destination and Initial Route Destination, will be reset to their default values (see Table 4-17, Node IP Options, and Table 4-22, SNMP Traps and Trap Dial-Out Options).
IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address needed to access the Ethernet port. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the port, which can be viewed or edited. **Clear** – Fills the IP address with zeros.
Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask associated with the IP address that is needed to access the Ethernet port. **000.000.000.000 – 255.255.255.255** – Set the Ethernet port's subnet mask. The range for each byte is 000 to 255. **Clear** – Fills the subnet mask associated with the IP address with zeros.

Table 4-23. Ethernet Management Options (2 of 2)

Default Gateway Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the IP address for the port's default gateway. It is used for packets that do not have a route. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the port, which can be viewed or edited (i.e., a router on the LAN). **Clear** – Fills the default gateway's IP address with zeros.
Proxy ARP
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether the FrameSaver unit will use the Proxy ARP (Address Resolution Protocol) technique, acting as the gateway to other FrameSaver devices in its management network when there is an ARP request for a device not on the Ethernet. **Enable** – Proxy ARP is enabled on the port so the FrameSaver unit will act as an agent for or gateway to other units in its management network. Using this technique, the FrameSaver unit returns its own MAC (Media Access Control) address in response to ARP requests when it recognizes that the destination IP address is in its subnet, but the device sending the ARP request is in another network. Packets sent to the FrameSaver unit's gateway address are forwarded to the appropriate device. **Disable** – The Proxy ARP technique will not be used by the unit; it will not act as an agent for other devices in its network.

Configuring the Communication Port

Select Communication Port from the Management and Communication menu to display or change the communication port configuration options (see Table 4-24, Communication Port Options).

Main Menu→Configuration→Management and Communication→ Communication Port

Table 4-24. Communication Port Options (1 of 5)

Port Use
Possible Settings: **Terminal, Net Link, Modem PassThru** Default Setting: **Terminal**
Assigns a specific use to the COM port. NOTE: If the Default IP Destination is set to COM (see Table 4-17, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The COM port is used for the asynchronous terminal connection. **Net Link** – The COM port is the network communications link to the IP network or IP device port. You cannot change Port Use to Net Link when the Modem PassThru feature is enabled. When you try, the `Cannot change Port Use – Modem PassThru is enabled` message is displayed. **Modem PassThru** – Available to the FrameSaver SLV 9626 only, the COM port is connected to the router's auxiliary (AUX) or console port so the router can be accessed via a dial-up connection to the unit. When this feature is active, a logical connection between the unit's modem and COM ports is made, and data received over the modem port is transmitted out the COM port to the router's AUX or console port. When an escape sequence (minus, minus, minus, with a minimum of 50 ms between each) is detected, the FrameSaver unit switches back to normal user interface operation.
Data Rate (Kbps)
Possible Settings: **9.6, 14.4, 19.2, 28.8, 38.4, 57.6, 115.2** Default Setting: **19.2**
Specifies the rate for the COM port in kilobits per second. **9.6 – 115.2 Kbps** – Sets the communication port speed.
Character Length
Possible Settings: **7, 8** Default Setting: **8**
Specifies the number of bits needed to represent one character. NOTE: Character length defaults to 8 and cannot be changed if Port Use is set to Net Link. **7** – Sets the character length to seven bits. **8** – Sets the character length to eight bits. Use this setting if using the COM port as the network communication link.

Table 4-24. Communication Port Options (2 of 5)

Parity
Possible Settings: **None, Even, Odd** Default Setting: **None**
Provides a method of checking the accuracy of binary numbers for the COM port. A parity bit is added to the data to make the "1" bits of each character add up to either an odd or even number. Each character of transmitted data is approved as error-free if the "1" bits add up to an odd or even number as specified by this configuration option. **None** – Provides no parity. **Even** – Makes the sum of all 1 bits and its corresponding parity bit always even. **Odd** – Makes the sum of all 1 bits and its corresponding parity bit always odd.
Stop Bits
Possible Settings: **1, 2** Default Setting: **1**
Determines the number of stop bits used for the COM port. **1** – Provides one stop bit. **2** – Provides two stop bits.
Ignore Control Leads
Possible Settings: **Disable, DTR** Default Setting: **Disable**
Specifies whether DTR is used. *Display Conditions* – This option does not apply to the FrameSaver SLV Router. **Disable** – Treats control leads as standard operation. **DTR** – Ignores DTR. This may be necessary when connecting to some PAD devices.
Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether a user ID and password (referred to as the login) is required in order to log on to the asynchronous terminal connected to the COM port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Requires a login to access the menu-driven user interface. **Disable** – Does not requires a login.

Table 4-24. Communication Port Options (3 of 5)

Port Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies level of user access privilege for an asynchronous terminal connected to the COM port. If a login is required for the port, the effective access level is determined by the user's access level. When a login is *not* required, the effective access level is determined by this option. NOTE: The effective access level is always the lowest one assigned to either the port or the user. For example, if the Port Access Level assigned is Level-2, but the User Access Level is Level-3, then only level-3 access will be permitted for the port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Level-1** – Allows full access and control of the device including monitoring, diagnostics, and configuration. The user can add, change, and display configuration options, and perform device testing. CAUTION: Before changing the communication port's access level to Level-2 or 3, make sure that either Telnet Session Access Level or the Modem Port's Port Access Level is set top Level-1 and at least one Login ID is set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. **Level-2** – Allows limited access and control of the device. The user can monitor and perform diagnostics, display status and configuration option information. **Level-3** – Allows limited access with monitoring control only. The user can monitor and display status and configuration screens only.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a user session is disconnected after a specified time of inactivity (no keyboard activity). *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Disconnects user session after the specified time of inactivity. **Disable** – Does not disconnect user session.
Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Specifies the number of minutes of inactivity that can elapse before the session is disconnected. *Display Conditions* – This option only appears when Port Use is set to Terminal. **1 – 60** – Sets the time from 1 to 60 minutes (inclusive).

Table 4-24. Communication Port Options (4 of 5)

IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies a unique IP address for accessing the unit via the COM port. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option only appears when Port Use is set to Net Link. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the COM port, which you can view or edit. **Clear** – Clears the IP address for the COM port and fills the address with zeros. When the IP Address is all zeros, the COM port uses the Node IP Address if one has been configured.
Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the unit. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option only appears when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the COM port, which you can view or edit. **Clear** – Clears the subnet mask for the COM port and fills the address with zeros. When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.
RIP
Possible Settings: **None, Standard_out** Default Setting: **None**
Specifies which Routing Information Protocol (RIP) is used to enable routing of management data between devices. *Display Conditions* – This option only appears when Port Use is set to Net Link. **None** – No routing is used. **Standard_out** – The device will send standard RIP messages to communicate routing information about other FrameSaver units in the network. Standard RIP messages received on this link are ignored. NOTE: The router must be configured to receive RIP on the port connected to the COM port, configured as the management interface (e.g., Cisco: **config-t, router RIP, int serial*x*, IP RIP Receive version 1, ctl-z WR**). To create this management interface, make sure that Node or COM port IP Information has been set up (see *Configuring Node IP Information* on page 4-74).

Table 4-24. Communication Port Options (5 of 5)

Link Protocol
Possible Settings: **PPP, SLIP** Default Setting: **PPP**
Specifies the link-layer protocol to be used. Only in effect when the COM port is configured as a network communication link (Port Use option is set to Net Link). *Display Conditions* – This option only appears when Port Use is set to Net Link. **PPP** – Point-to-Point Protocol. **SLIP** – Serial-Line Internet Protocol.

Configuring the Modem Port

Select Modem Port from the Management and Communication menu to configure the modem port (seeTable 4-25, Modem Port Options).

Main Menu→Configuration→Management and Communication→
Modem Port

Table 4-25. Modem Port Options (1 of 4)

Port Use
Possible Settings: **Terminal, Net Link** Default Setting: **Terminal**
Assigns a specific use to the modem port. NOTE: If the Default IP Destination is set to Modem (see Table 4-17, Node IP Options) and you change Port Use to Terminal, the Default IP Destination is forced to None. **Terminal** – The modem port is used for the asynchronous terminal connection. **Net Link** – The modem port is a network communications link to the IP network. You cannot change Port Use to Net Link when the Modem PassThru feature is enabled. When you try, the **`Cannot change Port Use – Modem PassThru is enabled`** message is displayed. See *Modem Operation* in Chapter 7, *Operation and Maintenance*, for more information about Modem PassThru operation.
Dial-In Access
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Controls whether external devices can dial-in to the system through the internal modem. This allows dial-in access by a remote terminal when Port Use is set to Terminal. When Port Use is set to Net Link, Dial-In Access must be set to Enable to allow an external NMS to dial in to the device. **Enable** – Dial-in access is allowed. Incoming calls are answered. **Disable** – Dial-in access is not allowed. Incoming calls are not answered. You cannot disable Dial-In Access when the Modem PassThru feature is enabled. When you try, the **`Cannot change Dial-In Access when Modem PassThru is enabled`** message is displayed. See *Modem Operation* in Chapter 7, *Operation and Maintenance,* for more information about Modem PassThru operation.

Table 4-25. Modem Port Options (2 of 4)

Login Required
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether a user ID and password (referred to as the login) is required in order to log on to the asynchronous terminal connected to the modem port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Requires a login to access the menu-driven user interface. **Disable** – Does not require a login.
Port Access Level
Possible Settings: **Level-1, Level-2, Level-3** Default Setting: **Level-1**
Specifies the level of user access privilege for an asynchronous terminal connected to the modem port. NOTE: The effective access level is always the lowest one assigned to either the port or the user. For example, if the Port Access Level assigned is Level-2, but the User Access Level is Level-3, then only Level-3 access will be permitted for the modem port. *Display Conditions* – This option only appears when Port Use is set to Terminal. **Level-1** – Allows full access and control of the device including monitoring, diagnostics, and configuration. The user can add, change, and display configuration options, save, and perform device testing. If Login Required is set to Enable, the effective access level is determined by the user’s access level. Otherwise, the access level is 1. CAUTION: Before changing the modem port’s access level to Level-2 or 3, make sure that either Telnet Session Access Level or the communications port’s Port Access Level is set to Level-1 and at least one Login ID are set to Level-1. Otherwise, access will be lost. If this occurs, you must reset the unit to the factory defaults and begin the configuration process again. **Level-2** – Allows limited access and control of the device. The user can monitor and perform diagnostics, display status and configuration option information. If Login Required is set to Enable, the effective access level is 2 for User ID access levels of 1 or 2. User IDs set to access Level-3 have only Level-3 access. **Level-3** – Allows limited access with monitoring control only. The user can only display and monitor status and configuration screens. If Login Required is set to Enable, the effective access level is 3 for all user IDs.
Inactivity Timeout
Possible Settings: **Enable, Disable** Default Setting: **Enable**
Determines whether a user session is disconnected after a specified time of inactivity (no keyboard activity). *Display Conditions* – This option only appears when Port Use is set to Terminal. **Enable** – Disconnects the user session after the specified time of inactivity. **Disable** – Does not disconnect the user session.

Table 4-25. Modem Port Options (3 of 4)

Disconnect Time (Minutes)
Possible Settings: **1 – 60** Default Setting: **10**
Determines the amount of lapsed time before disconnecting a user session in minutes. *Display Conditions* – This option only appears when: ■ Port Use is set to Terminal. ■ Inactivity Timeout is set to Enable. **1 – 60** – Sets the number of minutes allowed before the modem disconnects.
IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies a unique IP address for accessing the system via the modem port. This option is only in effect when the modem port is configured as a network communication link. *Display Conditions* – This option only appears when Port Use is set to Net Link. **001.000.000.000 – 223.255.255.255** – Shows the IP address for the modem port, which you can view or edit. **Clear** – Clears the IP address for the modem port and fills the address with zeros (i.e., 000.000.000.000). When the IP Address is all zeros, the modem port uses the Node IP Address if one has been configured.
Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the subnet mask needed to access the system. This option is only in effect when the modem port is configured as a network communication link. *Display Conditions* – This option only appears when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the modem port, which you can view or edit. **Clear** – Clears the subnet mask for the COM port and fills the address with zeros. When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.
Link Protocol
Possible Settings: **PPP, SLIP** Default Setting: **PPP**
Specifies the link-layer protocol to be used. This option is only in effect when the modem port is configured as a network communication link. *Display Conditions* – This option only appears when Port Use is set to Net Link. **PPP** – Point-to-Point Protocol. **SLIP** – Serial-Line Internet Protocol.

Table 4-25. Modem Port Options (4 of 4)

Alternate IP Address
Possible Settings: **001.000.000.000 – 223.255.255.255, Clear** Default Setting: **Clear** (000.000.000.000)
Specifies the alternate IP address for the modem port. If this configuration option is not configured (i.e., it is zero), the modem port's primary IP address is used when the alternate telephone directory is used for dial-out traps. *Display Conditions* – This option only appears when Port Use is set to Net Link. **001.000.000.000 – 223.255.255.255** – Shows the modem's alternate IP address, which you can view or edit. **Clear** – Clears the alternate IP address for the modem port and fills the address with zeros.
Alternate Subnet Mask
Possible Settings: **000.000.000.000 – 255.255.255.255, Clear** Default Setting: **000.000.000.000**
Specifies the alternate subnet mask needed to access the unit. Only in effect when the modem port is configured as a network communication link. *Display Conditions* – This option only appears when Port Use is set to Net Link. **000.000.000.000 – 255.255.255.255** – Shows the subnet mask for the modem port, which you can view or edit. **Clear** – Clears the subnet mask for the modem port and fills the address with zeros. When the node subnet mask is all zeros, the IP protocol creates a default subnet mask based upon the class of the IP address: Class A: 255.000.000.000, Class B: 255.255.000.000, or Class C: 255.255.255.000.

Configuring the Criteria for Automatic Backup

For units with an ISDN DBM, follow this menu selection sequence to specify whether and when automatic backup is allowed, and to configure timers that will control and terminate backup, or set delays (see Table 4-26, Auto Backup Criteria Options).

Main Menu→Configuration→Auto Backup Criteria

Table 4-26. Auto Backup Criteria Options (1 of 2)

Auto Backup
Possible Settings: **Enable, Disable** Default Setting: **Disable**
Determines whether backup for the access unit is automatically performed when the primary physical link or LMI, or a DLCI on a PVC connection fails, or when latency is exceeded. When enabled, the access unit automatically enables the Alternate Link configuration option, and establishes an alternate DLCI and EDLCI, rerouting traffic over the backup interface. (See Table 4-18, Management PVC Options, to configure the alternate DLCI and alternate EDLCI.) NOTE: Auto Backup cannot be enabled unless LMI Behavior is set to Independent (see Table 4-1, System Frame Relay and LMI Options). **Enable** – Reroutes traffic over the backup (alternate) interface. **Disable** – Does not reroute traffic over the backup interface.
DLCI Down Backup Activation Delay (sec)
Possible Settings: **0 – 3600** Default Setting: **0**
Specifies the number of seconds the unit will wait once a DLCI is declared down before it initiates backup. A DLCI is declared down when the DLCI changes to Inactive status in an LMI response, or when there is an LMI or physical link failure. When a delay is configured, the unit is more tolerant of network glitches, or repeated short outages, before going into backup, minimizing bouncing between network and backup services. **0 – 3600** – Specifies the amount of time for the delay.
DLCI Down Backup Activation Transition Threshold
Possible Settings: **1 – 10** Default Setting: **1**
Specifies how many times a primary destination DLCI transitions up or down during the DLCI Down Backup Activation Delay period before the unit initiates backup, provided the DLCI is active when the delay period ends. **1 – 10** – Specifies the number of transitions allowed between Active and Inactive status.
Backup Restoration Delay (sec)
Possible Settings: **0 – 3600** Default Setting: **0**
Specifies the number of seconds the unit will wait after all backup alarm conditions have cleared for a primary destination DLCI before the backup connection is terminated. **0 – 3600** – Specifies the amount of time for the delay.

Table 4-26. Auto Backup Criteria Options (2 of 2)

When Auto Backup Allowed
Possible Settings: **Always, Restrict** Default Setting: **Always**
Determines when backup for the access unit is allowed to occur. **Always** – No restrictions on backup. **Restrict** – Backup is restricted to the day and time selected in the following configuration options. Use this selection when the importance of the data that you are backing up is day/time dependent.
Backup Allowed: *Day* From *nn:nn*
Possible Settings: **00:00 – 23:00, None** Default Setting: **00:00**
Specifies the time that Auto Backup can begin for a selected day of the week in increments of 1 hour. *Day* is Monday through Sunday. **00:00 – 23:00** – Specifies the time of day that Auto Backup will start for this particular day. **None** – Auto Backup cannot occur on this day.
Backup Allowed: *Day* To *nn:nn*
Possible Settings: **00:00 – 24:00** Default Setting: **24:00**
Specifies the time that Auto Backup must end occurring for the selected day of the week in increments of 1 hour. *Display Conditions* – This option only appears if a start time was specified. **00:00 – 24:00** – Specifies the time of day that Auto Backup will stop for this particular day.

Configuring the FrameSaver SLV Router

5

This chapter includes the following:

FrameSaver SLV Router Overview

The FrameSaver SLV Router supports locally attached hosts or subnets and various customer premises distribution networks that contain IP forwarding devices or routers. The router is shipped as an 802.1d bridge, and it can be configured to simultaneously support IP routing and bridging of all non-IP protocols. The router maintains two routing tables to keep customer data and management data separate.

The router supports Internet Protocol (IP), specified in RFC 791, and Internet Control Message Protocol (ICMP), as specified in RFCs 792 and 950 (with exceptions). It acts as a router or gateway as defined in RFC 791.

The router has two interfaces:

- **Network Interface**

  Frame relay packets are transported over the T1 line using this interface.

- **Ethernet**

  This is a 10/100BaseT interface that automatically negotiates the rate. If all attached Ethernet devices support 100BaseT, the router defaults to 100BaseT. Otherwise, the router operates at 10BaseT. The interface has a unique MAC address.

  — In router mode, the router accepts on the Ethernet interface only those frames with its own MAC address or a broadcast or multicast MAC address.

  — In bridge mode, the router accepts all frames and forwards only ones for which the destination MAC address does not match an entry in the bridge table. This is the default setting.

NOTES:

— The configuration examples included in this chapter cover some common configurations, providing only a few of the possible scenarios.

— IP addresses used in the examples are for illustrative purposes only; they are not intended to be used when configuring your local network.

— Command syntax will vary based on your network setup.

— Configuration commands require an access level of Administrator-Config, and changes need to be saved when being configured to take effect.

For additional information, refer to:

- Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*, for details on the supported MIBs and RFCs.
- Appendix C, *Router CLI Commands, Codes, and Designations,* for specific commands and complete syntax.
- Appendix D, *Router Command Line Summaries and Shortcuts*, for specific command default settings and abbreviated command line syntax.

IP Routing

The router uses destination-based routing. IP routing tables are maintained for both the customer data and management data domains to specify how IP datagrams are forwarded. The router can support up to 32 entries in the data IP routing table, and up to 300 entries for the management IP routing table. When an IP address and subnet mask are assigned to an interface, an entry is automatically created in the IP routing table.

Address Resolution Protocol

The router supports Address Resolution Protocol (ARP), as specified in RFC 826. The router provides for 256 ARP table entries. The timeout for completed and uncompleted ARP table entries is configurable.

The Command Line Interface provides the ability to:

- Create up to 64 static ARP table entries to be retained across power cycles.
- Display the ARP table.
- Delete ARP table entries.
- Display and delete automatically added static ARP table entries by the DHCP server and relay functions. Refer to *Dynamic Host Configuration Protocol Server* on page 5-11.

Proxy ARP

The router supports Proxy ARP. Proxy ARP responses are based on the contents of the IP routing table for management traffic. The IP routing table for management traffic must have an entry for every host that is reachable on the Ethernet interface, including hosts for which the router will not forward packets because of IP filters. For additional information on filtering, refer to *IP Filtering* on page 5-15.

If an ARP request is received on one interface for an IP address that is reachable on the other interface, the router will respond with its own MAC address. Proxy ARP is enabled via the user interface. Refer to *Configuring Ethernet Management* in Chapter 4, *Configuration Options.*

Proxy ARP and NAPT cannot be enabled at the same time.

Interface Configuration

The following examples require that IP addresses have been assigned to the Ethernet and Serial interfaces, and that a passthrough PVC connection exists to Rtr-S0. Optionally you might also disable bridging.

In the following example, the Serial 0 sub-interface is shown as x. The valid range is 0–4,294,967,295.

▶ Procedure

To set up the router's interfaces:

1. If a Net1-FR1 DLCI does not exist:

   — Create one using the Network Circuit Records screen, then select CreatePVC.

   — When the **`Create PVC using DLCI Number?`** prompt appears, select a DLCI and press Enter.

   — When the **`Create Pass-Thru PVC Connection to:?`** prompt appears, enter **Rtr-S0**.

   — Save the configuration.

2. From the Main Menu screen, press Ctrl-a then Shift-r to access the router's Command Line Interface. Set the IP addresses of the interfaces.

   The following example commands:

   — Set the Ethernet interface address to 10.1.3.1

   — Set the Serial 0.*x* interface to 172.20.95.2

   — Disable bridging for both interfaces

   — Specify that messages for all IP addresses should be routed to the upstream router at 172.20.95.1

```
en
config t
int e 0
ip address 10.1.3.1 255.255.255.0
no bridge-group 1
int se 0.x
ip address 172.20.95.2 255.255.255.0
no bridge group 1
exit
ip route 0.0.0.0 0.0.0.0 172.20.95.1
save
exit
```

Network Address Translation

Network Address Translation (NAT) is used when a private network's internal IP addresses cannot be used outside the private network. IP addresses may be restricted for privacy reasons, or they may not be valid public IP addresses.

The router provides NAT as described in RFC 1631, The IP Network Address Translator (NAT). NAT allows hosts in a private (local) network to transparently access the external (public or global) network by using a block of public addresses. Static mapping enables access to selected local hosts from the outside using these external IP addresses.

Traditional NAT and Network Address Port Translation (NAPT) are supported. When both NAT and NAPT are enabled, one-to-one NAT mapping is performed by translating a range of assigned public IP addresses to a similar-sized pool of private addresses, followed by many-to-one NAPT bindings. Up to 254 IP addresses can be allocated for NAT usage.

IP Options Processing

The NAT and NAPT functions handle and process the IP datagrams with options set as described below. No command is available to set IP options.

The router does not process (and drops) any IP datagrams with the following IP options:

- Loose source and record route (type 131)
- Strict source and record route (type 133)
- Security (type 130)
- Stream ID (type 136)

The router does process IP datagrams with the following IP options, but does not provide its IP address or timestamp information in the response message:

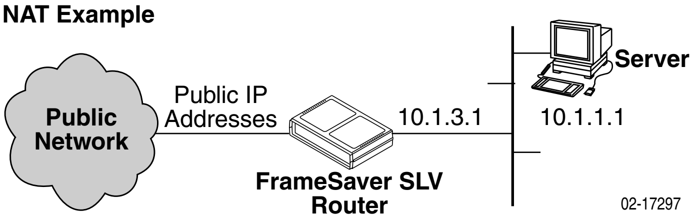
- Record route (type 7)
- Timestamp (type 68)

Applications Supported by NAT

The router supports the following applications and protocols:

- FTP
- HTTP
- Ping
- RealPlayer
- Telnet
- TFTP

NAT Configuration Example



In this NAT example:

- NAT is used for one-to-one mapping of addresses.
- The Ethernet interface is in the private address space and the network interface is in public address space. With NAT enabled, a single global PVC is used to access the public network.
- When using NAT, the network interface must be numbered because the Ethernet interface is configured within the private address space.
- The next hop router (default gateway) for the clients is the Ethernet IP address of the router, 10.1.3.1.
- There are four private IP addresses configured on the Ethernet side of the router with NAT static mappings to four public IP addresses.

NAT Mapping Public IP Addresses	Private IP Addresses
192.128.22.28	10.1.3.2
192.128.22.29	10.1.3.3
192.128.22.30	10.1.3.4
192.128.22.31	10.1.3.5

▶ Procedure

To set up NAT:

1. From the Main Menu screen, press Ctrl-a then Shift-r to access the router's Command Line Interface. Enter the following commands:

   ```
   en
   config t
   ip nat inside source static 10.1.3.2 192.128.22.28
   ip nat inside source static 10.1.3.3 192.128.22.29
   ip nat inside source static 10.1.3.4 192.128.22.30
   ip nat inside source static 10.1.3.5 192.128.22.31
   ```

2. Enable NAT on interfaces with the following commands (where *x* is the number configured for the sub-interface):

   ```
   interface ethernet 0
   ip nat inside
   interface serial 0.x
   ip nat outside
   ```

3. Save the configuration and exit the CLI:

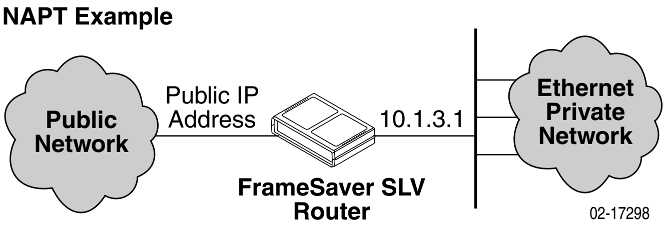
   ```
   save
   exit
   ```

Network Address Port Translation

Network Address Port Translation (NAPT) allows multiple clients in a local network to simultaneously access remote networks using a single IP address. This benefits telecommuters and SOHO (Small Office/Home Office) users that have multiple clients in an office running TCP/UDP applications. NAPT is sometimes referred to as PAT (Port Address Translation).

NAPT provides a many-to-one mapping and uses one public address to interface numerous private users to an external network. All hosts on the global side view all hosts on the local side as one Internet host. The local hosts continue to use their corporate or private addresses. When the hosts are communicating with each other, the translation is based on the IP address and the IP port numbers used by TCP/IP applications. Only TCP/UDP applications can access the public network.

NAPT Configuration Example



In this NAPT example the router is configured for NAPT using:

- A single public IP address. Multiple public addresses can be used.
- A public network. NAPT can also be used between private networks.
- An access list. A pool can also be used, instead or in addition.

NAPT Mapping Public IP Address	Private IP Addresses
172.20.95.2:zzzz	10.1.3.2:zzzz
172.20.95.2:yyyy	10.1.3.3:yyyy
172.20.95.2:xxxx	10.1.3.4:xxxx

▶ Procedure

To set up NAPT:

1. From the Main Menu screen, press Ctrl-a then Shift-r to access the router's Command Line Interface.

2. Set up an access list. The following command specifies a list that includes addresses 10.1.3.1 through 10.1.3.254:

   ```
   access-list 1 permit 10.1.3.0 0.0.0.255
   ```

3. Enable NAPT. The following command specifies that inside address translation is performed on the addresses in Access List 1, and the outside address is the address of the Serial interface 0, sub-interface *x*:

   ```
   ip nat inside source list 1 interface se 0.x overload
   ```

4. Specify which interface uses inside (private) and which uses outside (public) IP addresses:

   ```
   int ethernet 0
   ip nat inside
   int serial 0.x
   ip nat outside
   ```

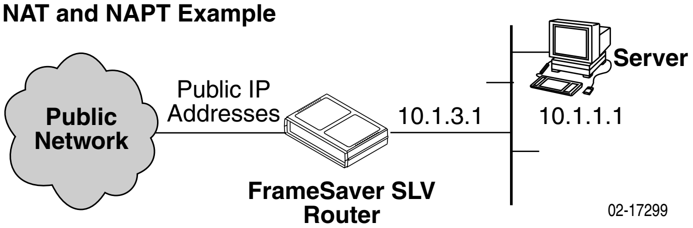
5. Save the configuration and exit the CLI:

   ```
   save
   exit
   ```

NAT and NAPT Configuration Example

The router can be configured for NAT and NAPT simultaneously.

NAT and NAPT Example



In this NAT and NAPT example:

- Multiple workstations in the private address space can use NAPT, and the server in the private address space can use NAT.
- The server may need NAT to send more than TCP/UDP traffic, or accommodate multiple types of inbound traffic types.

  For example, a Web server that uses FTP for maintenance needs access from the public address side for HTTP and FTP using NAT.

▶ Procedure

To configure the router for both NAPT and NAT:

1. Set up the router for NAPT. See *Network Address Port Translation* on page 5-8.
2. Set up a static address for any host not using NAPT:

   ```
   ip nat inside source static 10.1.1.1 155.22.17.1
   ```

Dynamic Host Configuration Protocol Server

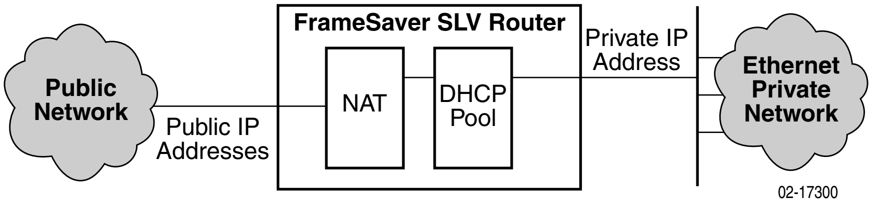
The router provides a Dynamic Host Configuration Protocol (DHCP) Server feature as specified in RFC 2131, Dynamic Host Configuration Protocol, and RFC 2132, DHCP Option and BOOTP Vendor Extensions. DHCP is the protocol used for automatic IP address assignment.

DHCP setup considerations:

- The range of IP addresses to be used by the DHCP server must be configured. The maximum number of clients is 253.
- The DHCP server is not activated until one IP address and subnet mask are assigned to the Ethernet interface.
- DHCP server and DHCP relay functions cannot be enabled at the same time.
- When the DHCP IP address range is changed, all binding entries, automatically added routes, and ARP table entries for the clients configured with the old address range are removed.
- When the DHCP Server is enabled, there can be only one IP address configured for the Ethernet interface.
- The IP address for the next hop router provided to the hosts in the DHCP reply must be configured.
- The minimum and maximum lease time settings can be configured.
- The subnet mask can be configured along with the IP address range (optional).
- The DHCP server domain name can be configured (optional).
- The Domain Name Server (DNS) IP address can be configured (optional).

DHCP Server with NAT Configuration Example

NAT with DHCP Server



In this DHCP Server with NAT example:

- The clients are using dynamic IP address assignment and use the Ethernet interface of the router as the next hop router (default gateway).
- The DHCP server assigns private IP addresses which are converted to public IP addresses by NAT.
- The network interface must be numbered.
- The router is configured as the DHCP server giving the private IP addresses to the clients.
- The Ethernet interface is in private address space. NAT is used for one-to-one mapping of addresses.

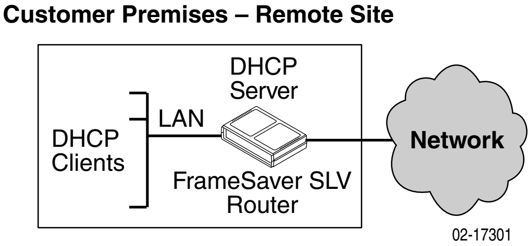
Public IP Addresses for NAT	Private IP Addresses
192.128.22.1	10.1.3.2
192.128.22.2	10.1.3.3
. . .	. . .
192.128.22.nnn	10.1.3.nnn

The command line syntax for this example, where *x* is the number configured for the sub-interface, is:

```
ip nat pool public 192.128.22.1 netmask 255.255.255.0
access-list 1 permit 10.1.1.0 0.0.0.255
ip nat inside source list 1 pool public
interface ethernet 0
ip nat inside
interface serial 0.x
ip nat outside
```

DHCP Server at Remote Site Configuration Example

DHCP Server at Remote Site



In this DHCP Server at the remote site example:

- The DHCP clients send IP address requests to the specified DHCP server.
- The router is the DHCP server and provides IP addresses to DHCP clients on the local Ethernet segment.
- This example creates a pool of 254 reusable IP addresses.

The command line syntax for this example is:

```
ip dhcp pool pool17
network  155.1.3.0  255.255.255.0
default-router 155.1.3.254
```

DHCP Relay Agent

The router provides the capability of serving as a DHCP Relay Agent, as specified in RFC 2131, Dynamic Host Configuration Protocol. The router provides the capability to enable and disable the DHCP Relay Agent and to configure the IP address of the DHCP server to which the DHCP requests are to be sent.

The DHCP server assigns an IP address to the end-user system. When DHCP Relay is enabled, it is possible to limit the number of DHCP clients. The router's IP Routing table and ARP table are automatically updated. The DHCP relay agent in the router should be used when there is a DHCP server at the customer's headquarters or central site.

DHCP relay agent setup considerations include the following:

- DHCP server IP address must be configured.
- DHCP relay must be enabled; i.e., both the server address and the interface closest to the server are configured.
- The number of DHCP clients is limited to 1–253.
- DHCP server and DHCP relay functions cannot be enabled at the same time.
- NAT and DHCP relay cannot be enabled at the same time.
- With DHCP relay enabled, the router sends the DHCP request to the DHCP server.

Router Security

The router offers security via the following:

- Filtering can be enabled or disabled for inbound and/or outbound traffic:
  - Ethertype
  - ICMP Message Type, Code
  - IP Protocol Type: TCP, UDP, or ICMP
  - TCP/UDP Ports
  - IP Source/Destination IP Address
- Always enabled:
  - Land Bug Prevention
  - Smurf Attack Prevention

IP Router Filtering

Router filtering does not apply when the router is in bridge-only mode. By default, filtering is disabled on the router. Filtering provides security advantages on LANs by restricting traffic on the network. A filter consists of a set of rules applied to a specific interface to indicate whether a packet received or sent on that interface is forwarded or discarded.

Filters are configured in general router configuration mode, then applied to the Ethernet or frame relay network interface. Filters are applied to traffic in either the transmit or receive direction on that interface.

There is one filter access list per interface, per direction, with a maximum of 33 rules per list. For IP filters, all rules with a source host IP address are applied first; all rules with a destination host IP address are applied next. The remaining filters are applied in the order in which they were configured.

Bridge Filtering

Bridge filtering does not apply when the router is in router-only mode. When bridging is enabled, separate ethertype filters are applied to the Ethernet and frame relay interfaces. They are applied to traffic in either the transmit or receive direction on that interface, with one filter access list per interface, per direction. There is a maximum of 16 rules per list. Each rule in the access list allows the user to filter a single ethertype or range of ethertypes.

MAC frames can be filtered based on the:

- SNAP Ethernet field in the 802.2 and 802.3 header.
- Protocol type field in the DIX Ethernet header.

For ethertype filters, the rules are applied in the order in which they were configured.

IP Filtering

When NAT is enabled and the IP filters are active, filtering is done on the Ethernet port: upstream first, then downstream.

- Upstream: From the client to the server
- Downstream: From the server to the client

Land Bug Prevention

The router drops all packets received on a network PVC interface or the Ethernet interface when the Source IP address is the same as the Destination IP address.

Smurf Attack Prevention

The router ignores requests to send an ICMP echo reply to the broadcast address and ICMP echo requests with a destination of the broadcast address.

Provisioning the Router Interface

The FrameSaver SLV Router defaults to bridge mode. Routing without bridging, and simultaneous routing and bridging, are also options.

Use the bridge command from the router's CLI to configure the bridge and routing attributes. Also, enter an Ethernet IP address and a DHCP IP address.

Refer to Appendix C, *Router CLI Commands, Codes, and Designations*, for command line syntax and information about CLI commands. For a list of default settings, see *CLI Command Default Settings* in Appendix D, *Router Command Line Summaries and Shortcuts*.

Configuring the Router Using Terminal Emulation

The CLI is available via a Telnet session or a direct connection over the router's COM port to a VT100-compatible terminal or a PC running a terminal emulation program. You access the CLI through the router's menu-driven user interface. From the Main Menu, press Shift-r to access the CLI.

Verify the required terminal settings:

- Data rate is set to 19.2 Kbps (19200 bps).
- Character length is set to 8.
- Parity is set to None.
- Stop bits is set to 1.
- Flow control is set to Off or None.

Uploading and Downloading the Router Configuration Via the CLI

Use the **show configuration** command to output command strings needed to restore the current running configuration.

Output from the show configuration command can be captured to a text file using most terminal emulation programs. Once the text file is captured, the router can be placed in configuration mode. The text file can then be fed back to configure the router.

Security and Logins

6

This chapter includes the following:

Limiting Access

The FrameSaver unit provides access security on the following interfaces:

- Asynchronous terminal
- Telnet
- FTP
- SNMP

Up to two direct or Telnet sessions can be active at any given time; that is, you can have two simultaneous Telnet sessions, or one Telnet session and one active asynchronous terminal session, or two simultaneous asynchronous terminal sessions.

Controlling Asynchronous Terminal Access

Direct asynchronous terminal access to the menu-driven user interface can be limited by:

- Requiring a login.
- Assigning an access level to the port or interface.

An asynchronous terminal can be connected to the unit’s COM (communications) port or its modem port.

▶ Procedure

To limit asynchronous terminal access to the menu-driven user interface:

1. Select the appropriate port options.

   Main Menu → Configuration → Management and Communication → Communication Port

   Main Menu → Configuration → Management and Communication → Modem Port

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login* on page 6-12.
Limit the effective access level to Level-3 or Level-2	Port Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the port (e.g., if a user has a Level-1 login and Level-2 port access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow Level-1 users to configure the unit, keep the access at Level-1.

NOTE:

See *Resetting the Unit and Restoring Communication* in Chapter 8, *Troubleshooting*, should you be locked out inadvertently.

3. Save your changes.

If connecting an asynchronous terminal to the unit's:

- COM port – See *Configuring the Communication Port* in Chapter 4, *Configuration Options,* for more information about the communication (COM) port.
- Modem port – See *Setting Up Call Directories for Trap Dial-Out* and *Configuring the Modem Port* in Chapter 4, *Configuration Options,* for additional information.

Limiting Dial-In Access via the Modem Port

The modem port is already configured for dial-in and asynchronous terminal access; these are the default settings.

To limit dial-in access via the modem port, disable the Dial-In Access configuration option.

> *Main Menu→Configuration→Management and Communication→ Modem Port*

See *Configuring the Modem Port* in Chapter 4, *Configuration Options,* for more information about modem port options.

Controlling ISDN Access

FrameSaver units with the built-in DBM limit access through the following methods:

- *ISDN Call Security*
- *Disabling ISDN Access*

ISDN Call Security

The FrameSaver unit uses the Caller Identification Method to screen calls and avoid accidental or intentional disruption of network traffic. The answering DBM only accepts calls with valid calling number identifiers or phone numbers.

When the ISDN DBM interface is enabled and Caller Identification Method is set to Caller ID, the DBM takes advantage of ISDN services for network backup and Calling Number Identification Service (CNIS) to provide backup security. ISDN assures the integrity of calling party identifiers. The DBM uses the calling party identifier to identify the calling unit and switches PVC connections as specified by the user. No additional security is required.

When the ISDN DBM interface is enabled and Caller Identification Method is set to Proprietary, the DBM queries the originating unit for its Local Phone Number to identify the calling unit. If the returned number is in one of the unit's Inbound Calling IDs, the call is accepted. If not, or if the queried unit does not respond within five seconds, the unit drops the call.

See Caller Identification Method in Table 4-11, ISDN Link Profile Options, in Chapter 4, *Configuration Options*, for additional information.

Disabling ISDN Access

▶ Procedure

To disable ISDN access:

1. Select the ISDN Physical options.

   Main Menu→Configuration→ISDN→Physical

2. Set Interface Status to Disable.
3. Save your change.

See *Configuring the ISDN DBM Interface* in Chapter 4, *Configuration Options,* for more information about ISDN BRI or PRI DBM configuration options.

Controlling Telnet or FTP Access

The FrameSaver unit provides several methods for limiting access via a Telnet or FTP session. Telnet or FTP access can be on a standard management link or on a service provider's troubleshooting (TS) management link.

Limiting Telnet Access

Telnet access can be limited by:

- Disabling Telnet access completely.
- Requiring a login for Telnet sessions that are not on the TS Access Management Link.
- Assigning an access level for Telnet sessions.
- Disabling TS Access Management Link access.

To limit Telnet access via a service provider's troubleshooting management link, see *Limiting Telnet or FTP Access Over the TS Access Management Link* on page 6-8.

▶ Procedure

To limit Telnet access when the session is **not on** the TS Access Management Link:

1. Select the Telnet and FTP Session options.

   Main Menu→Configuration→Management and Communication→ Telnet and FTP Sessions

2. Set the following configuration options, as appropriate.

To . . .	**Set the configuration option . . .**
Disable Telnet access	Telnet Session to Disable.
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login* on page 6-12.
Assign an access level	Session Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the Telnet session (e.g., if a user has a Level-1 login and Level-2 telnet access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow users to configure the unit, keep the access at Level-1.

3. Save your changes.

See *Configuring Telnet and/or FTP Session Support* in Chapter 4, *Configuration Options,* for more information about setting Telnet configuration options.

Limiting FTP Access

FTP access can be limited by:

- Disabling FTP access completely.
- Requiring a user ID and password to login.
- Limiting FTP bandwidth.

▶ Procedure

To limit FTP access when the session is **not on** the TS Access Management Link:

1. Select the Telnet and FTP Session options.

   Main Menu→Configuration→Management and Communication→
   Telnet and FTP Sessions

2. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable FTP	FTP Session to Disable.
Require a login	Login Required to Enable. **NOTE:** User ID and password combinations must be defined. See *Creating a Login* on page 6-12. If you want to allow users to configure the unit or perform file transfers, including downloads, keep the access at Level-1. Level-1 access is required to download software to the unit, or to upload or download configuration files. Level-3 is sufficient for NMS access for SLV historical information.
Limit bandwidth for FTP	FTP Max Transfer Rate to a rate less than the network line speed, typically less than or equal to the CIR. This method is not recommended if SLV reports are desired since FTP is required to generate the reports.

3. Save your changes.

See *Configuring Telnet and/or FTP Session Support* in Chapter 4, *Configuration Options,* for more information about setting FTP configuration options.

Limiting Telnet or FTP Access Over the TS Access Management Link

▶ Procedure

To limit Telnet or FTP access when the session is **on** the TS Access Management Link:

1. Select the Telnet and FTP Session options.

   Main Menu→Configuration→Management and Communication→ Telnet and FTP Sessions

2. Disable Telnet Session and/or FTP Session, as appropriate.
3. Return to the Management and Communication menu, and select Node IP.
4. Set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Disable access via the TS Access Management Link	TS Access Management Link to None.
Assign an access level to the TS Access Management Link	TS Access Management Link's Access Level to Level-2 or Level-3. **NOTE:** Regardless of a user's login access level, a user cannot operate at a level higher than the access level specified for the session (e.g., if a user has a Level-1 login and Level-2 telnet access has been set, the Level-1 user can only operate as a Level-2 user). If you are going to allow users to configure the unit, keep the access at Level-1.

5. Save your changes.

See *Configuring Telnet and/or FTP Session Support* or *Configuring Node IP Information* in Chapter 4, *Configuration Options,* for more information about these configuration options.

Controlling SNMP Access

The FrameSaver unit supports SNMP Version 1, which provides limited security through the use of community names. There are three methods for limiting SNMP access:

- Disabling SNMP access.
- Assigning SNMP community names and the access type.
- Assigning IP addresses of those NMSs that can access the unit.

Disabling SNMP Access

When the SNMP access is disabled, the FrameSaver unit will not respond to SNMP messages.

▶ Procedure

To disable SNMP access:

1. Select the General SNMP Management options.

   Main Menu→Configuration→Management and Communication→ General SNMP Management

2. Disable the SNMP Management option.
3. Save your change.

See *Configuring General SNMP Management* in Chapter 4, *Configuration Options,* for more information about General SNMP Management configuration options.

Assigning SNMP Community Names and Access Levels

The FrameSaver unit supports the SNMP protocol and can be managed by an SNMP manager. SNMP manager access can be limited by:

- Assigning the SNMP community names that are allowed to access the FrameSaver unit's Management Information Base (MIB).
- Specifying the type of access allowed for each SNMP community name.

Whenever an SNMP manager attempts to access an object in the MIB, the community name must be supplied.

▶ Procedure

To assign SNMP community names and access types:

1. Select the General SNMP Management options.

   Main Menu→Configuration→Management and Communication→ General SNMP Management

2. Set the following configuration options, as appropriate.

To . . .	**Set the configuration option . . .**
Assign SNMP community names	Community Name 1 and Community Name 2 to a community name text, up to 255 characters in length.
Assign the type of access allowed for the SNMP community names	Name 1 Access and Name 2 Access to Read or Read/Write.

3. Save your changes.

See *Configuring General SNMP Management* in Chapter 4, *Configuration Options,* for more information about General SNMP Management configuration options.

Limiting SNMP Access Through IP Addresses

An additional level of security is provided by:

- Limiting the IP addresses of NMSs that can access the FrameSaver unit.
- Performing validation checks on the IP address of SNMP management systems attempting to access the FrameSaver unit.
- Specifying the access allowed for the authorized NMS when IP address validation is performed.

The SNMP NMS Security Options screen provides the configuration options that determine whether security checking is performed on the IP address of SNMP management systems attempting to communicate with the unit.

Make sure that SNMP Management is set to Enable.

Menu selection sequence:
Main Menu → Configuration → Management and Communication → General SNMP Management → SNMP Management: Enable

See *Configuring General SNMP Management* in Chapter 4, *Configuration Options,* for more information about SNMP management configuration options.

▶ Procedure

To limit SNMP access through IP addresses:

1. Select the SNMP NMS Security options:

   Main Menu→Configuration→Management and Communication→ SNMP NMS Security

2. Select and set the following configuration options, as appropriate.

To . . .	Set the configuration option . . .
Enable IP address checking	NMS IP Validation to Enable.
Specify the number (between 1 and 10) of SNMP management systems that are authorized to send SNMP messages to the FrameSaver unit	Number of Managers to the desired number.
Specify the IP address(es) that identifies the SNMP manager(s) authorized to send SNMP messages to the unit	NMS *n* IP Address to the appropriate IP address.
Specify the access allowed for an authorized NMS when IP address validates is performed	Access Level to Read or Read/Write.

3. Save your changes.

See *Configuring SNMP NMS Security* in Chapter 4, *Configuration Options,* for more information about SNMP NMS Security configuration options.

Creating a Login

A login is required if security is enabled**.** Security is enabled by the configuration options Login Required for the communication port, modem port, and Telnet Login Required or FTP Login Required for a Telnet or FTP Session.

Up to six login ID/password combinations can be created using ASCII text, and each login must have a specified access level. Logins must be unique and they are case-sensitive.

▶ Procedure

To create a login record:

1. Select Administer Logins.

   Main Menu→Control→Administer Logins

2. Select New, and set the following configuration options, as appropriate.

In the field . . .	**Enter the . . .**
Login ID	ID of 1 to 10 characters.
Password	Password from 1 to 10 characters.
Re-enter password	Password again to verify that you entered the correct password into the device.
Access Level	Access level: 1, 2, or 3. ■ Level-1 – User can add, change, and display configuration options, save, and perform device testing. ■ Level-2 – User can monitor and perform diagnostics, display status and configuration option information. ■ Level-3 – User can only monitor and display status and configuration screens. **CAUTION:** Make sure at least one login is set up for Level-1 access or you may be inadvertently locked out.

NOTE:

See *Resetting the Unit and Restoring Communication* in Chapter 8, *Troubleshooting*, should you be locked out inadvertently.

3. Save your changes.

   When Save is complete, the cursor is repositioned at the Login ID field, ready for another entry.

See *Configuring SNMP NMS Security* in Chapter 4, *Configuration Options,* for more information about security configuration options.

Modifying a Login

Logins are modified by deleting the incorrect login and creating a new one.

Deleting a Login

▶ Procedure

To delete a login record:

1. Select Administer Logins.

   Main Menu→Control→Administer Logins

2. Page through login pages/records using the PgUp or PgDn function keys until the login to be deleted is displayed.

3. Select Delete.

4. Save your deletion.

   When the deletion is complete, the number of login pages/records reflects one less record, and the record before the deleted record reappears.

   Example:
   Page 2 of 4 is changed to Page 2 of 3.

Controlling Router CLI Access

The FrameSaver SLV 9126-II Router can be managed from an NMS using SNMP, or from the router's command line interface (CLI). There are two methods to access the command line interface:

- Local access at the router through the COM port, or
- Access via a Telnet session.

  Telnet access defaults to Administrator level. If the current login is at the Operator level, only Operator level access is available for the session. Telnet access is always enabled.

The router accepts one CLI login session at a time and is configured at the factory without a default login ID and password. To provide login security to the system, configure a login ID and password.

When a local console connection is first established, a login prompt appears. If the Device Name field has been configured via the Control menu *(Control Menu→System Information)*, the login prompt displays the device name. For example, a device name of Largo is shown as:

```
Largo>
```

See *Creating a Login* on page 6-12 for security information for each Login ID.

Access Levels (Command Modes)

There is one login ID and several levels of privileges for the router's CLI. Your user account can be configured with one user name and different passwords for:

- **Operator**. The Operator has read-only access to display device information with no modification permission and limited access to diagnostic functions. With a device name of Largo, the prompt appears as Largo>.
- **Administrator**. The Administrator has several levels of access to the router's CLI. The # sign in the following prompts indicates Administrator access level.

Display Prompt with Device Name of Largo	Administrator Access Levels
Largo #>	Standard (same as Operator)
Largo(config) #	Configuration
Largo(config-if) #	Configuration Interface
Largo(config-subif) #	Configuration Sub-Interface
Largo(config-dhcp) #	Configuration DHCP Pool

Refer to Appendix C, *Router CLI Commands, Codes, and Designations*, for access level details for each command line entry.

Changing Access Levels

The Operator and Administrator have the same Login ID with different passwords for their access level. To determine the level of access for a session, refer to *Access Levels (Command Modes)* on page 6-14.

After accessing the router's CLI:

- You can access the Administrator access level by entering:

  ```
  enable
  ```

- The router's defaults to no password required. To require a password to access the Administrator access level, enter:

  `enable password` *password*

  Once saved, the router responds with a prompt to enter a password for Administrator access. This command is in effect until **`no enable password`** [*password*] is entered and saved.

- You can end the current Administrator access level by entering:

  ```
  exit
  ```

  This command results in ending the current Administrator access level session. Exit may need to be entered several times to reach Operator level and/or end the session.

- You can end the Administrator access level by entering:

  ```
  end
  ```

  This command results in ending the Administrator access level session and returning immediately to Operator level.

For further details, refer to *Chapter 5, Configuring the FrameSaver SLV Router,* and Appendix C, *Router CLI Commands, Codes, and Designations*.

Operation and Maintenance

7

This chapter includes the following:

Displaying System Information

Use the Identity screen to view identification information about the FrameSaver unit. This information is useful if you are purchasing additional or replacement units and/or making firmware upgrades.

Main Menu→Status→Identity

View this field . . .	To find the . . .
System Name	Domain name for this SNMP-managed node (up to 255 ASCII characters).
System Contact	Contact person for this SNMP-managed node.
System Location	Physical location for this SNMP-managed node.
NAM	
NAM Type	Type of unit installed, referred to as a network access module, or NAM (i.e., T1 FR NAM). This card type is supported by the SNMP SysDescr Object.
Hardware Revision	Unit's hardware version. Format *nnnn-nnx* consists of a 4-digit number, followed by two digits and one alphabetic character.
Current Software Revision	Software version currently being used by the unit. Format *nn.nn.nn* consists of a 6-digit number that represents the major and minor revision levels.
Alternate Software Revision	Software version that has been downloaded into the unit, but has not yet been implemented. Format is the same as for the Current Software Revision. ■ **`In Progress`** indicates that the flash memory is currently being downloaded. ■ **`Invalid`** indicates that no download has occurred or the download was not successful
Serial Number	Unit's 7-character serial number.
Ethernet MAC Address	Media Access Control (MAC) address assigned to the Ethernet port during manufacturing.

View this field . . .	To find the . . .
ISDN DBM	
Card Type	The type of dial backup module installed, ISDN-BRI or ISDN-PRI, if applicable. ■ If an unsupported DBM is installed, **`Unsupport`** displays. ■ If the DBM has failed, **`Failed`** displays.
Software Revision	Software version currently being used by the FrameSaver unit's DBM. Format *nn.nn.nn* consists of a 6-digit number that represents the major and minor revision levels. For an ISDN-PRI DBM, **`None`** displays because the DBM does not have loaded software; it runs from the NAM's software.
Hardware Revision	FrameSaver DBM's hardware version. Format *nnnn-nnx* consists of a 4-digit number, followed by 2 digits and 1 alphabetic character.

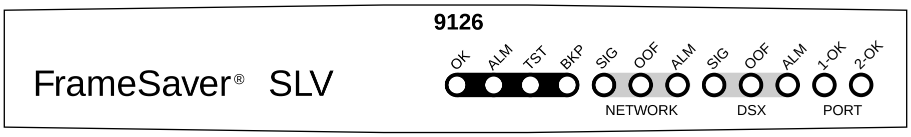
Viewing LEDs and Control Leads

FrameSaver SLV faceplates include LEDs (light-emitting diodes) that provide status on the unit and its interfaces. These faceplates are shown in the following sections.

The Display LEDs and Control Leads feature allows you to monitor a remote unit; it is useful when troubleshooting control lead problems. The Display LEDs and Control Leads screen shows the appropriate interfaces for the unit, with the appropriate status highlighted.

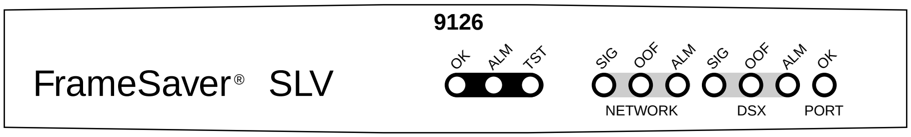
FrameSaver SLV 9126 LEDs and Control Leads

The FrameSaver SLV 9126-A1 unit's faceplate includes LEDs (light-emitting diodes) that provide status on the FrameSaver unit, its network interface, DSX-1 interface, and DTE interface.



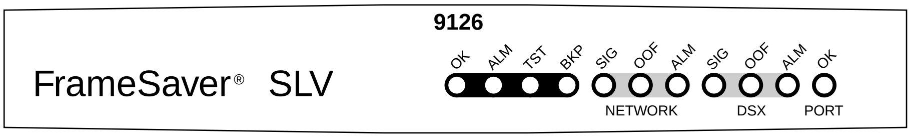
00-16182-01

The FrameSaver SLV 9126-A2-201's faceplate includes LEDs that provide status on the FrameSaver unit, its network interface, DSX-1 interface, and DTE interface.



02-17142a

The FrameSaver SLV 9126-II's and FrameSaver SLV 9126-II Router's faceplates include LEDs that provide status on the FrameSaver unit, its backup mode, its network interface, DSX-1 interface, and DTE interface. The PORT LED refers to the user data port on the CSU/DSU, and the Ethernet port on the router.

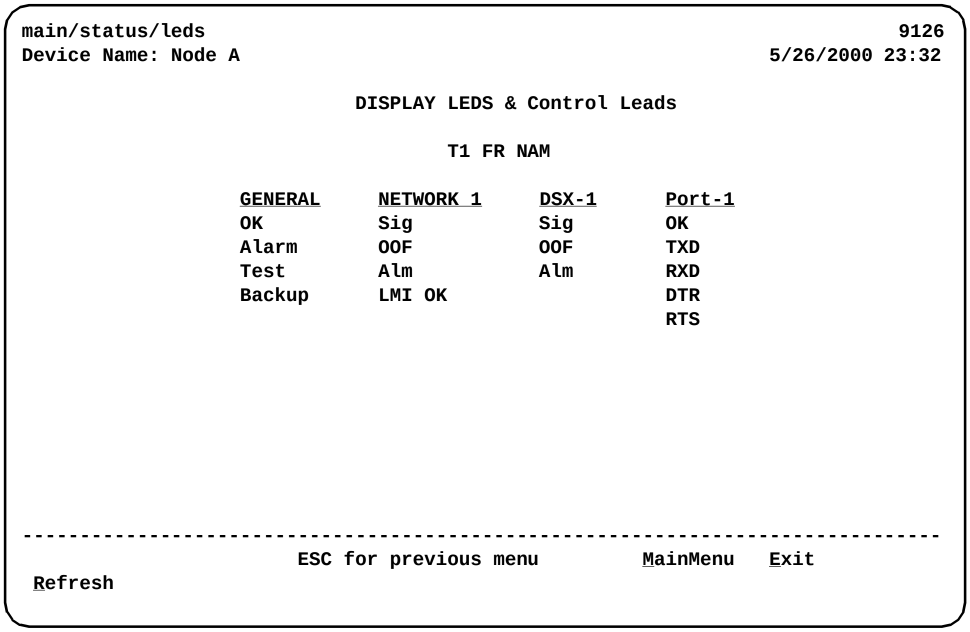


02-17142

To access the Display LEDs and Control Leads screen:

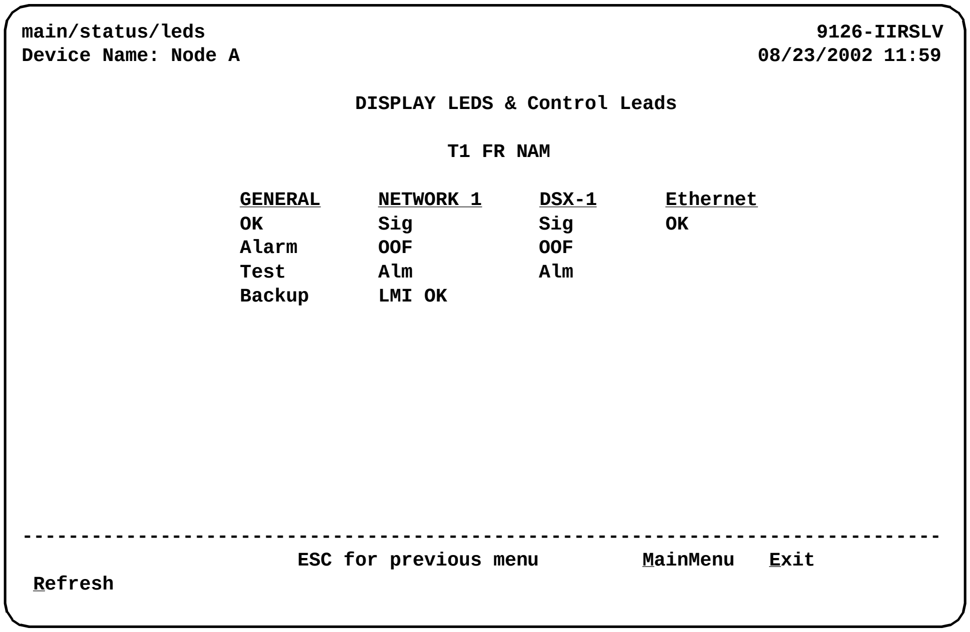
Main Menu → Status → Display LEDs and Control Leads

Display LEDs & Control Leads Screen for a FrameSaver SLV 9126



```
main/status/leds                                                              9126
Device Name: Node A                                                5/26/2000 23:32

                            DISPLAY LEDS & Control Leads

                                    T1 FR NAM

                   GENERAL     NETWORK 1     DSX-1      Port-1
                   OK          Sig           Sig        OK
                   Alarm       OOF           OOF        TXD
                   Test        Alm           Alm        RXD
                   Backup      LMI OK                   DTR
                                                        RTS










--------------------------------------------------------------------------------
                       ESC for previous menu         MainMenu   Exit
 Refresh
```

Display LEDs & Control Leads Screen for a FrameSaver SLV 9126-II Router

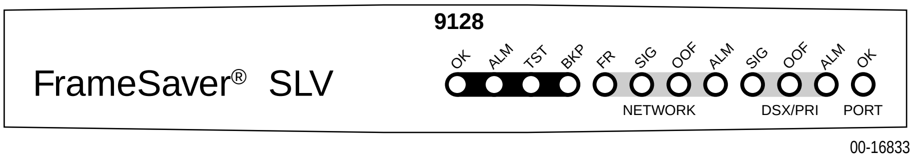


```
main/status/leds                                                       9126-IIRSLV
Device Name: Node A                                               08/23/2002 11:59

                            DISPLAY LEDS & Control Leads

                                    T1 FR NAM

                   GENERAL     NETWORK 1     DSX-1      Ethernet
                   OK          Sig           Sig        OK
                   Alarm       OOF           OOF
                   Test        Alm           Alm
                   Backup      LMI OK











--------------------------------------------------------------------------------
                       ESC for previous menu         MainMenu   Exit
 Refresh
```

Refresh the screen to view control lead transitions. LED and control lead descriptions are in the sections that follow.

FrameSaver SLV 9128-II LEDs and Control Leads

The FrameSaver SLV 9128-II faceplate includes 12 LEDs (light-emitting diodes) that provide status on the FrameSaver unit, its network interface, DSX/PRI, and DTE interface. The FrameSaver SLV 9128-II, with an Ethernet port, faceplate is shown below.

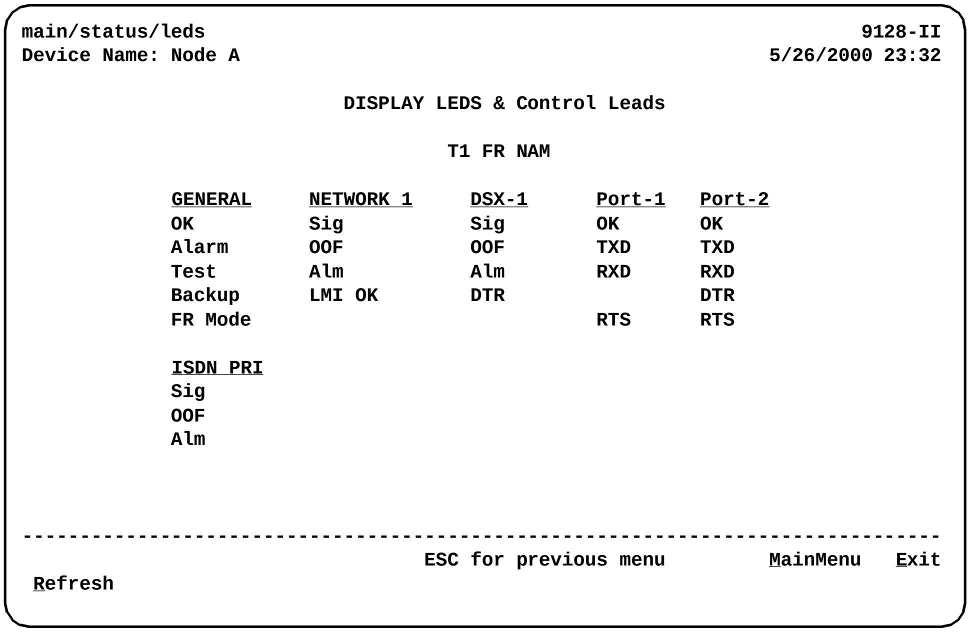


To access the Display LEDs and Control Leads screen:

Main Menu → Status → Display LEDs and Control Leads

The following example shows the screen for a FrameSaver SLV 9128-II with an ISDN PRI DBM installed.

Display LEDs & Control Leads Screen for a FrameSaver SLV 9128-II



```
main/status/leds                                                      9128-II
Device Name: Node A                                           5/26/2000 23:32

                            DISPLAY LEDS & Control Leads

                                     T1 FR NAM

             GENERAL     NETWORK 1     DSX-1      Port-1   Port-2
             OK          Sig           Sig        OK       OK
             Alarm       OOF           OOF        TXD      TXD
             Test        Alm           Alm        RXD      RXD
             Backup      LMI OK        DTR                 DTR
             FR Mode                              RTS      RTS

             ISDN PRI
             Sig
             OOF
             Alm



--------------------------------------------------------------------------------
                                   ESC for previous menu         MainMenu   Exit
 Refresh
```

Refresh the screen to view control lead transitions. LED and control lead descriptions are in the sections that follow.

LED Descriptions

Table 7-1, General Status LEDs, identifies the alarms that cause the Alarm LED to light. See Table 7-2, Network, DSX, or PRI Interface LEDs, for network, DSX-1, and PRI interface LED information, Table 7-3, User Data Port LED (CSU/DSUs Only), for user data port interface LED information, and Table 7-4, Ethernet Port LED (Routers Only) for Ethernet interface LED information.

Table 7-1. General Status LEDs (1 of 2)

Label	Indiction	Color	What It Means
OK[1]	Power and Operational Status	Green	ON – FrameSaver unit has power and it is operational. OFF – FrameSaver unit is in a power-on self-test, or there is a failure.
ALM	Operational Alarm (Fail)	Red	ON – FrameSaver unit has just been reset, or an error or fault has been detected. Error/fault/alarm conditions: ■ Alarm Indication Signal (AIS) ■ CTS Down ■ DBM BRI Card Failure ■ DBM Download Failed ■ DLCI Down ■ DTR Down ■ Ethernet Link Down ■ Exceeded Error Rate (EER) ■ Internal Modem Failed ■ ISDN Network Failed ■ LMI Down ■ Loss of Signal (LOS) ■ Network Communication Link Down ■ Out of Frame (OOF) ■ Power Supply/Fan Failure ■ Primary or Secondary Clock Failed ■ Self-Test Failed ■ SLV Latency Exceeded ■ SLV Timeout ■ Suboptimal Link Rate ■ Two Level-1 Users Accessing Device ■ Yellow Alarm Signal

[1] When an ISDN BRI DBM is installed, if the OK LED comes on then goes off during power recycling, the ISDN BRI DBM may have failed.

[2] On the Display LEDs & Control Leads screen for the Model 9128-II only, FR Mode is On or Off. When On (highlighted), the FrameSaver unit is in Frame Relay mode.

Table 7-1. General Status LEDs (2 of 2)

Label	Indiction	Color	What It Means
ALM *(cont'd)*	Operational Alarm (Fail)	Red	ON – FrameSaver unit has just been reset, or an error or fault has been detected. Alarms appear on the System and Test Status screen. See Table 7-8, Health and Status Messages, for additional information. OFF – No failures have been detected.
TST	Test Mode	Yellow	ON – Loopback or test pattern is in progress, initiated locally, remotely, or from the network. OFF – No tests are active.
BKP	Backup	Yellow	ON – FrameSaver unit is in Backup mode; that is, the backup link has been established, and backup is in progress through the specified Alternate Destination Link. OFF – FrameSaver unit is not in Backup mode. Blinking ON and OFF – Alternate Destination Link is being established, but no data has been passed.
FR Mode [2] *(Model 9128-II only)*	Frame Relay Mode	Multi-colored	Yellow – LMI is down on the FrameSaver SLV 9128-II. Green – LMI is up on the FrameSaver SLV 9128-II.

[1] When an ISDN BRI DBM is installed, if the OK LED comes on then goes off during power recycling, the ISDN BRI DBM may have failed.

[2] On the Display LEDs & Control Leads screen for the Model 9128-II only, FR Mode is On or Off. When On (highlighted), the FrameSaver unit is in Frame Relay mode.

Table 7-2. Network, DSX, or PRI Interface LEDs

Label	Indication	Color	What It Means
SIG	Signal	Green	ON – A recoverable signal is present on the Network/DSX/PRI interface. OFF – The signal cannot be recovered from the Network/DSX/PRI interface. An LOS condition exists.
OOF	Out of Frame	Yellow	ON – At least one OOF was detected during the sampling period. OFF – No OOFs were detected during the sampling period.
ALM	Alarm	Yellow	ON – An alarm condition is present on the network/DSX/PRI interface. Current alarm conditions: ■ Loss of Signal (LOS) ■ Loss of Frame (LOF) ■ Out of Frame (OOF) ■ Excessive Error Rate (EER) ■ Yellow Alarm Signal ■ Alarm Indication Signal (AIS) OFF – No alarm condition is present on the Network/DSX/PRI interface.

Table 7-3. User Data Port LED (CSU/DSUs Only)

Label	Indication	Color	What It Means
OK [1]	Operational Status	Green	ON – The interchange circuits for the port are in the correct state to transmit and receive data. OFF – The port is idle. Occurs if the port is disabled, or if the port is configured to monitor DTR and/or RTS and the lead(s) is not asserted.

[1] The FrameSaver SLV 9128-II only has one OK LED even though it has two user data ports. If either port is enabled and active, the LED is on. If both ports are enabled and one of the ports is inactive, the LED is off.

Table 7-4. Ethernet Port LED (Routers Only)

Label	Indication	Color	What It Means
OK	Operational Status	Green	ON – The Ethernet port is transmitting and receiving. OFF – The port is idle.

Control Lead Descriptions

See Table 7-2, Network, DSX, or PRI Interface LEDs, for descriptions of these leads. See Table 7-3, User Data Port LED (CSU/DSUs Only), to interpret the user data port OK control lead. The LED descriptions and control lead descriptions are the same.

In addition to these LEDs, additional control leads can be monitored through the Display LEDs and Control Leads screen. These indicators show the current state of each control lead and what they indicate when they are highlighted; that is, in the On state. They are described in Table 7-5, Additional Control Leads.

Table 7-5. Additional Control Leads

Label	Indication	What It Means
Network Interface		
LMI OK	LMI Operational Status	LMI is operating successfully on the first frame relay link on the network interface.
User Data Port		
TXD	Transmit Data	Data is being sent to the far-end device.
RXD	Receive Data	Data is being received from the far-end device.
DTR	Data Terminal Ready	Shows the current state of the DTR control lead. This indicator should always be on.
RTS	Request to Send	Shows the current state of the RTS control lead. This indicator should always be on.

Device Messages

These messages appear in the messages area at the bottom of the screens. All device messages are listed in alphabetical order.

Table 7-6. Device Messages (1 of 6)

Message	What It Indicates	What To Do
Access level is *n*, Read-only.	User's access level is 2 or 3; user is not authorized to change configurations.	No action needed.
Already Active	Test selected is already running.	■ Allow test to continue. ■ Select another test. ■ Stop the test.
Blank Entries Removed	New had been selected from the Administer Logins screen, no entry was made, then Save was selected.	■ No action needed. ■ Reenter the Login ID, Password, and Access Level.
Cannot Delete Trap Manager	Delete was selected from the Management PVCs Options screen, but the PVC had been defined as a trap destination.	No action needed, or configure another path for traps and try again.
Cannot Save – no Level 1 Login IDs	Security was being set up, but all the logins were assigned either Level-2 or Level-3 access.	Set up at least one login with Access Level-1 so the unit can be configured.
Command Complete	Configuration has been saved or all tests have been aborted.	No action needed.
Connection Refused *(Seen at an FTP terminal.)*	Two menu-driven user interface sessions are already in use when a Telnet session was attempted.	Wait and try again.
Destination Not Unique	Destination entered is already being used.	Enter another destination indicator.
DLCI in connection. Delete connection first	User tried to delete a DLCI that was part of a connection.	■ No action needed, or ■ Delete the connection, then delete the DLCI.
DLCI Number Already Exists	The DLCI number entered on the DLCI Record Entry screen has already been created so is not unique.	Enter another DLCI number.
DLCI Number Reserved	User tried to designate a special troubleshooting DLCI.	No action is needed.

Table 7-6. Device Messages (2 of 6)

Message	What It Indicates	What To Do
Duplicate DLCI Number	DLCI number entered is not unique for the frame relay link.	No action needed; previous contents of the DLCI number field is restored.
File Transfer Complete *(Seen at an FTP terminal.)*	A file transfer was performed successfully.	Switch to the newly downloaded software. See *Changing Software* on page 7-79.
File Transfer Failed – Invalid file *(Seen at an FTP terminal.)*	A file transfer was attempted, but it was not successful.	■ Try again, making sure you type the filename correctly. ■ Exit the FTP session, or download another file. See *Changing Software* on page 7-79.
Invalid – Already Active	A test was already in progress when it was selected.	No action needed.
Invalid Character (*x*)	A non-valid printable ASCII character has been entered.	Reenter information using valid characters.
Invalid date: must be mm/dd/yyyy	A non-valid date was entered on the System Information screen.	Reenter the date in the month/day/4-digit year format.
Invalid date and/or time	A non-valid date or time was entered on the System Information screen. The date does not exist (e.g., February 30th).	Reenter the date in the month/day/4-digit year format and/or time in the hour:minutes:seconds format.
Invalid – Link Already Active	Start was selected for a Test Call, but the selected frame relay link is currently in use.	Wait until the link is available and try again.
Invalid – No ISDN Channels Available	Start was selected for a Test Call, but all supported ISDN channels are currently in use.	Wait until a channel is available and try again.
Invalid – No Test Call Active	Stop was selected for a Test Call and no test call is active on the selected link. This can occur when the test is ended because the link is needed for an active connection, but the PVC Test screen has not yet been updated to Start.	Start the Test Call again when the connection is Inactive again.
Invalid time: must be hh:mm:ss	A non-valid system time was entered on the System Information screen.	Reenter the time in the hour:minutes:seconds format.

Table 7-6. Device Messages (3 of 6)

Message	What It Indicates	What To Do
Invalid Password	Login is required and an incorrect password was entered; access is denied.	■ Try again. ■ Contact your system administrator to verify your password.
Invalid Test Combination	A conflicting loopback or pattern test was in progress when Start was selected to start another test, or was active on the same or another interface when Start was selected.	■ Wait until other test ends and message clears. ■ Cancel all tests from the Test screen (Path: main/test). ■ Stop the test from the same screen the test was started from.
Limit of six Login IDs reached	An attempt to enter a new login ID was made, and the limit of six login/password combinations has been reached.	■ Delete another login/password combination. ■ Reenter the new login ID.
Limit of Mgmt PVCs reached	New was selected from the PVC Connection Table and the maximum number of management PVCs has already been created.	■ Do not create the management PVC. ■ Delete another management PVC, and try again.
Limit of PVC Connections reached	New was selected from the PVC Connection Table and the maximum number of PVCs has already been created.	■ Do not create the PVC connection. ■ Delete another PVC connection, and try again.
Name Must be Unique	Name entered for a management PVC has been used previously.	Enter another 4-character name for the logical/management link.
No Destination Link DLCIs Available	New was selected from the PVC Connection Table, but even though DLCIs are available to form a connection, no DLCIs are available on the network link, which is a suitable PVC Destination.	Configure additional DLCIs for the network link and try again.
No DLCIs available for connection	New was selected from the PVC Connection Table, but all configured DLCIs have been connected.	No action needed, or configure more DLCIs and try again.
	New was selected from the Management PVCs option screen, but all Link/DLCI pairs have been connected.	Configure more network and/or Port-1 Links/DLCIs pairs and try again.

Table 7-6. Device Messages (4 of 6)

Message	What It Indicates	What To Do
No DLCIs Available for Mgmt PVC	New was selected from the Management PVCs option screen, but all configured DLCIs have been connected.	Configure more network and/or Port-1 DLCIs and try again.
No DLCIs Defined	DLCI Records was selected from an interface's Configuration Edit/Display menu, and no DLCI Records have been created for this interface.	Select New and create a DLCI record.
No more DLCIs allowed	New or CopyFrom was selected from an interface's DLCI Records configuration screen, and the maximum number of DLCI Records had already been reached.	Delete a DLCI, then create the new DLCI Record.
No Primary Destination Link DLCIs Available	New or Modify was selected from the PVC Connection Table, but even though DLCIs are available to form a connection, no DLCIs are available on the network link, which is a suitable Primary PVC Destination.	Configure additional DLCIs for the network link and try again. If a network DLCI has been entered as a Source DLCI: 1. Change the Source DLCI to a user data port DLCI. 2. Enter the network DLCI as the PVC's Primary Destination.
No Security Records to Delete	Delete was selected from the Administer Login screen, and no security records had been defined.	■ No action needed. ■ Enter a security record.
Password Matching Error – Re-enter Password	Password entered in the Re-enter Password field of the Administer Logins screen does not match what was entered in the Password field.	■ Try again. ■ Contact your system administrator to verify your password.
Permission Denied *(Seen at an FTP terminal.)*	A file transfer was attempted, but the: ■ User did not have Level 1 security. ■ Wrong file was specified when the **put** command was entered. ■ User attempted to upload a program file from the unit.	■ See your system administrator to get your security level changed. ■ Try again, entering the correct file with the **put** command. ■ Enter the **put** command instead of a **get** command; you can only transfer files to the unit, not from it. See *Upgrading System Software* on page 7-77.

Table 7-6. Device Messages (5 of 6)

Message	What It Indicates	What To Do
Please Wait	Command takes longer than 5 seconds.	Wait until message clears.
Port Inactive *(FrameSaver SLV 9128-II only)*	The port is disabled, or it supports synchronous data when a DTE Loopback was started.	No action is needed.
Resetting Device, Please Wait ...	Yes (or y) was entered in the *Reset COM Port usage* field of the System Paused menu.	No action needed.
Save Cancelled *(FrameSaver SLV 9128-II only)*	Changes were made on the Easy Install screen, but when it came to saving the changes, the Esc key was pressed or No was entered in response to the **Save Changes?** prompt.	No action is needed.
Test Active	No higher priority System and Test Status messages exist, and a test is running.	■ Contact service provider if test initiated by the network. ■ Wait until the test ends and message clears. ■ Cancel all tests from the Test screen (Path: main/test). ■ Stop the test from the same screen the test was started from.
User Interface Already in Use	Two Telnet sessions are already in use when an attempt to access the menu-driven user interface through the COM port is made. IP addresses and logins of the users currently accessing the interface are also provided.	■ Wait and try again. ■ Contact one of the IP address user and request that they log off.
User Interface Idle	Previously active session is now closed/ended, and access via the COM port is now available.	Log on to the FrameSaver unit.
	Session has been ended due to timeout.	No action needed.

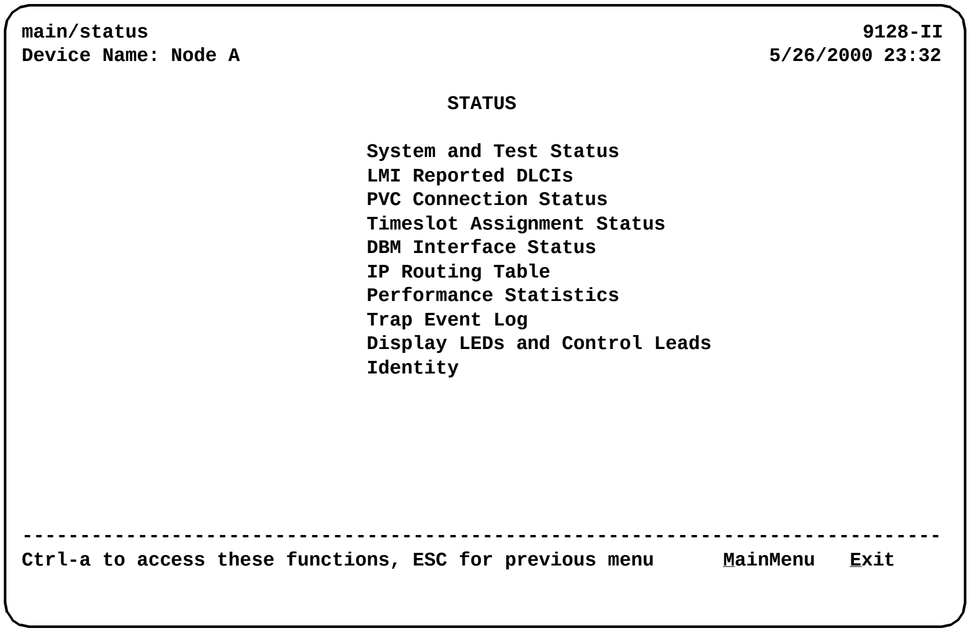
Table 7-6. Device Messages (6 of 6)

Message	What It Indicates	What To Do
Value Out of Range	CIR entered for the DLCI is a number greater than the maximum allowed.	Enter a valid CIR (0 – 64000).
	Excess Burst Size entered for the DLCI is a number greater than the maximum allowed.	Enter a valid Excess Burst Size (0 – 1536000).
	DLCI Number entered is less than 16 or greater than 1007.	Enter a valid number (16 – 1007).

Status Information

Status information is useful when monitoring the FrameSaver unit. The following illustration shows the Status menu for a FrameSaver SLV 9128-II with the ISDN DBM feature installed.

Status Menu Example



```
main/status                                                              9128-II
Device Name: Node A                                              5/26/2000 23:32

                                     STATUS

                              System and Test Status
                              LMI Reported DLCIs
                              PVC Connection Status
                              Timeslot Assignment Status
                              DBM Interface Status
                              IP Routing Table
                              Performance Statistics
                              Trap Event Log
                              Display LEDs and Control Leads
                              Identity






--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

DBM Interface Status will not appear on the menu if the unit does not have the optional ISDN DBM feature.

NOTE:

Status messages contained in the following sections are in alphabetical order.

System and Test Status Messages

System and test status information is selected from the Status menu.

Main Menu→Status →System and Test Status

The following information is included on this screen:

- Self-Test Results Messages (Table 7-7)
- Last System Reset Date and Time
- Health and Status Messages (Table 7-8)
- Test Status Messages (Table 7-9)

Self-Test Results Messages

One of these self-test result messages appears in the Self-Test Results field at the top of the System and Test Status screen.

Table 7-7. Self-Test Results Messages

Message	What It Indicates	What To Do
Failure *xxxxxxxx*	An internal failure occurred (*xxxxxxxx* represents an 8-digit hexadecimal failure code used by service personnel). Record the failure code before resetting the unit; otherwise, the error information will be lost.	1. Record the failure code. 2. Reset the unit. 3. Contact your service representative.
Passed	No problems were found during power-on or reset.	No action needed.

Last System Reset Date and Time

This field indicates the last time the FrameSaver unit was reset. It appears after the Self-Test Results field at the top of the System and Test Status screen.

- Date is in mm/dd/yyyy format (month/day/year).
- Time is in mm:ss format (minutes:seconds).

Health and Status Messages

The following table provides Health and Status messages that apply to the FrameSaver unit.

Table 7-8. Health and Status Messages (1 of 7)

Message	What It Indicates
AIS at DSX-1	An Alarm Indication Signal (AIS) is received by the DSX-1 interface. AIS is an unframed, all ones signal.
AIS at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	An Alarm Indication Signal (AIS) is received by the ISDN PRI interface. AIS is an unframed, all ones signal. Only appears when a PRI dial backup module (DBM) is installed. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. The ISDN network is transmitting an AIS.
AIS at Network 1	An Alarm Indication Signal (AIS) is received by the network interface. AIS is an unframed, all ones signal. Possible reasons include: ■ Upstream FrameSaver unit is transmitting AIS (keep-alive signal). ■ The network is transmitting an AIS.
Auto-Configuration Active	Auto-Configuration feature is active, which allows automatic configuration and cross-connection of DLCIs as they are reported by the network LMI.
Back-to-Back Mode Active	The operating mode has been configured for back-to-back operation (*Main Menu→ Control → Change Operating Mode).* The FrameSaver unit can be connected to another FrameSaver unit without a frame relay switch between them. This feature is useful for product demonstrations or for a point-to-point configuration using a leased line.
Backup Active	Backup has been established and data is flowing over the alternate DLCI.
CTS down to Port-1 Device	The user data port CTS control lead on the FrameSaver unit is off.
DBM BRI Card Failed *(ISDN BRI DBM only)*	One or more of the access unit's integrated circuit chips has failed to internally loop data through the dial backup unit BRI circuit.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with the user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Management Link DLCI.

Table 7-8. Health and Status Messages (2 of 7)

Message	What It Indicates
DBM Download Required *(ISDN BRI DBM only)*	A download attempt was interrupted and failed to complete. The NAM software and DBM software are incompatible.
DCLB Active, *[Interface]*	A V.54 Loopback is active on the specified interface.
DLCI *nnnn* Down, *frame relay link*[1,2]	The DLCI for the specified frame relay link is down.
DTE External LB Active, Port-*n*	A Data Terminal Loopback is running on the specified user data port.
DTE Init. Ext LB Active, Port-*n*	The DTE has initiated an external DTE Loopback on the specified user data port.
DTPLB Active, Port-2	A Data Terminal Payload Loopback (DTPLB) is active on the synchronous user data port.
DTR Down from Port-1 Device	The DTR control lead from the device connected to the user data port is deasserted.
EER at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	The error rate of the received ISDN network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing and a PRI dial backup module (DBM) is installed. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.
EER at Network 1	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.
Ethernet Link Down *(FrameSaver SLV 9126-II or 9128-II)*	The Ethernet port is enabled, but communication between the management system and the unit is not currently possible on the port.
Internal Modem Failed	The unit's internal modem failed to pass the self-test.
ISDN Active	An ISDN call is active.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with the user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Management Link DLCI.

Table 7-8. Health and Status Messages (3 of 7)

Message	What It Indicates
ISDN Link Profile Disabled *ISDN Link Name*	An ISDN backup call could not be made because the ISDN link profile specified Link Name is disabled (*Main Menu→ Configuration→ ISDN→ Link Profiles)*.
ISDN Link Profile Invalid, *ISDN Link Name*	No phone numbers have been specified in the ISDN link profile (specified by *ISDN Link Name*).
ISDN Network Failed (Active/Idle)	An ISDN network failure was detected when: ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode.
LatExceed*IP_ Address,* COS*x,*DLCI*nnnn*[1]	An IP SLV Latency Threshold has been exceeded for the specified COS of the path. *IP_Address* is the IP address of the path endpoint, COS*x* is the Class of Service ID associated with the path, and *nnnn* is the DLCI which contains the path.
Link Down Administratively, *frame relay link*[2]	The specified frame relay link has been disabled by the unit due to LMI Behavior conditions or LMI Protocol on another link is in a failed state.
Link Profile Disabled, *ISDN Link Name*	An ISDN backup call could not be made because the specified link profile was disabled.
LLB Active, *[Interface]*	A network Line Loopback (LLB) is active on the specified interface.
LMI Discovery in Progress, *frame relay link*[2]	Local Management Interface protocol discovery is in progress to determine which protocol will be used on the specified frame relay link.
LMI Down, *frame relay link*[2]	The Local Management Interface(s) has been declared down for the specified frame relay link. ■ For an individual ISDN link, the message appears when LMI has been declared down on the link. ■ For a multilink aggregate link, the message appears when LMI has been declared down on all constituent links of the frame relay multilink.
LOS at DSX-1	A Loss of Signal (LOS) condition is detected on the DSX-1 interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. Possible reasons include: ■ DSX-1 cable problem. ■ No signal being transmitted from the DTE.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with the user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Management Link DLCI.

Table 7-8. Health and Status Messages (4 of 7)

Message	What It Indicates
LOS at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	A Loss of Signal (LOS) condition is detected on the ISDN PRI interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. Only appears when a dial backup module (DBM) is installed. Possible reasons include: ■ DBM cable problem. ■ T1 facility problem.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%. Possible reasons include: ■ Network cable problem. ■ No signal is being transmitted at the far-end FrameSaver unit. ■ T1 facility problem.
Monitor Pttn. Active, DLCI *nnnn*, *frame_relay_link*[1,2]	The unit is monitoring a test pattern on the specified DLCI on the specified frame relay link.
Monitor *Pttn* Active, *[Interface]*	A Monitor Pattern test is active on the specified interface using a selected pattern. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Network Com Link Down	The communication link for the COM port is down, and the COM port is configured for Net Link.
Network Initiated ISDN BRI Test Active *(ISDN BRI DBM only)*	An ISDN test has been initiated by the ISDN BRI network and it is currently active.
OOF at DSX-1	An Out of Frame (OOF) condition is detected on the DSX-1 interface. Possible reasons include: ■ Incompatible framing format between the DTE and the FrameSaver unit. ■ DSX-1 cabling problem.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with the user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Management Link DLCI.

Table 7-8. Health and Status Messages (5 of 7)

Message	What It Indicates
OOF at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	An Out of Frame (OOF) condition is detected on the ISDN PRI interface. An OOF is declared when two out of four frame synchronization bits are in error. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. Possible reasons include: ■ Incompatible framing format between the ISDN network and the FrameSaver unit. ■ ISDN network cabling problem. ■ ISDN network problem.
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface. Possible reasons include: ■ Incompatible framing format between the network and the FrameSaver unit. ■ Network cabling problem. ■ T1 facility problem.
Path*IP_ Address* Down, DLCI*nnnn*[1]	A path on the network interface is unavailable. *IP_Address* is the IP address of the path endpoint, and *nnnn* is the DLCI which contains the path.
PLB Active, *[Interface]*	A Payload Loopback (PLB) is active on the specified interface.
Power Supply/Fan Alarm *(9000 Series Access Carrier only)*	The power supply output voltage has dropped below the specified tolerance level required for the system. Or the fan tray is not operating properly.
Primary Clock Failed	A failure of the primary clock source configured for the unit is detected and the secondary clock is providing the timing for the unit. This condition clears when the configured primary clock is restored.
Primary & Secondary Clocks Failed	A failure of the primary and secondary clock sources configured for the unit are detected and the internal clock is providing timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link*[1,2]	A PVC Loopback is active on the specified DLCI on the frame relay link.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with the user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Management Link DLCI.

Table 7-8. Health and Status Messages (6 of 7)

Message	What It Indicates
RLB Active, *[Interface]*	A network Repeater Loopback (RLB) is active on the specified interface.
Secondary Clock Failed	A failure of the secondary clock source configured for the unit is detected and the internal clock is providing the timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.
Send Pattern Active, DLCI *nnnn*, *frame_relay_link*[1,2]	A Send Pattern test is currently active on the specified DLCI on the specified frame relay link.
Send *Pttn* Active, *[Interface]*	A Send Pattern test is active on the specified interface using a selected test pattern. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
SLV Latency Exceeded, DLCI *nnnn*, *frame relay link*[1, 2, 3]	The measured latency of SLV communication responses from the remote unit on this DLCI is excessive, so the DLCI has been declared unsuitable for normal multiplexed PVC operation (DLCI Type is set to Multiplexed).
SLV Timeout, DLCI *nnnn*, *frame relay link*[1, 2, 3]	An excessive number of SLV communication responses from the remote FrameSaver SLV unit have been missed on the specified multiplexed DLCI; the DLCI is not suitable for user data. When a hardware bypass capable device has been detected at the other end of the PVC and this condition occurs, only user data for EDLCI 0 will be transmitted while this condition exists. When an ISDN DBM is present, this message only appears for individual and aggregate multilink frame relay links, not constituent links of a frame relay multilink.
Suboptimal Link Rate, *frame relay link*[2] *(ISDN DBM only)*	The specified frame relay multilink has failed to achieve the configured Maximum Link Rate for the link. This message appears for multilink aggregate frame relay links if LMI is down on any of its constituent links.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with the user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Management Link DLCI.

Table 7-8. Health and Status Messages (7 of 7)

Message	What It Indicates
Timeslot Discovery in Progress, Network 1	Time slot discovery is currently taking place to determine the time slots that will be used for frame relay traffic on the network interface. This message only appears when the Time Slot Discovery option is enabled (*Main Menu→ Configuration→ Time Slot Assignment→ Frame Relay Network Assignments)* and an LMI failure is detected on the network interface's frame relay link.
Two Level-1 Users Accessing Device	Two Level 1 users are already using the menu-driven user interface; only two sessions can be active at one time.
Test Call Active, *ISDN Link Name*	A test call is active on the specified frame relay link, the link being the ISDN Link Name assigned in the ISDN Link Profile. This message would only appear for models with the built-in DBM.
Yellow at DSX-1	A yellow alarm signal is received on the DSX-1 interface. DTE has detected a LOS or OOF condition.
Yellow at ISDN PRI (Active/Idle) *(ISDN PRI DBM only)*	A yellow alarm signal is received on the ISDN network interface. ■ Active – Backup call was in progress. ■ Idle – DBM was in Idle mode. Indicates a possible cable problem.
Yellow at Network 1	A yellow alarm signal is received on the network interface. Possible reasons include: ■ Network cable problem. ■ T1 facility problem.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with the user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Management Link DLCI.

Test Status Messages

These test messages appear in the right column of the System and Test Status screen. You have the option of allowing the test to continue or aborting the test. See *Chapter 8, Troubleshooting,* for more information on tests, including how to start and stop them.

Table 7-9. Test Status Messages (1 of 2)

Message	What It Indicates
DCLB Active, *frame_relay_link*[1] *or* DCLB Active, Port-2	A Data Channel V.54 Loopback (DCLB) is active on the specified frame relay link, or Port-2.
DTE External LB Active, Port-*n*	An external DTE Loopback is active on the user data port.
DTE Init. Ext LB Active, Port-*n*	An external DTE Loopback is active on the user data port.
DTPLB Active, Port-*n*	A Data Terminal Payload Loopback (DTPLB) is active on the user data port.
Lamp Test Active	The Lamp Test is active, causing the LEDs on the faceplate to flash on and off.
LLB Active, *Interface*[2]	A network Line Loopback (LLB) is active on the specified network, DSX-1, or ISDN PRI interface.
No Test Active	No tests are currently running.
PLB Active, *Interface*[2]	A Payload Loopback (PLB) is active on the specified network, DSX-1, or ISDN PRI interface.
PVC Loopback Active, DLCI *nnnn*, *frame_relay_link*[1,3]	A PVC Loopback is active on the specified DLCI for the frame relay link.
RLB Active, *Interface*[2]	A network Repeater Loopback (RLB) is active on the specified network or DSX-1 interface.
Send *Pttn* Active, *Interface*[2]	A Send Pattern test is active on the specified interface. This test cannot be activated on user data ports that have Port Use set to Frame Relay.

[1] *frame relay link* is one of the following:

- Net1-FR1. The frame relay link specified for the network interface, Network 1.
- Port-*n* for a 1-slot unit, or S*s*Port-*n* for a NAM in a multislot housing (the frame relay link associated with the specified user data port in the specified slot).
- *ISDN Link Name* on a non-network ISDN DBM interface.

[2] *Interface* is one of the following:

- Network 1
- DSX-1
- Port-*n*
- ISDN, BRI or PRI

[3] *nnnn* indicates a DLCI number of 16 through 1007.

Table 7-9. Test Status Messages (2 of 2)

Message	What It Indicates
Monitor *Pttn* Active, *Interface*[2]	A Monitor Pattern test is active on the specified interface. This test cannot be activated on user data ports that have Port Use set to Frame Relay.
Network Initiated ISDN BRI Test Active	An ISDN test has been started by the ISDN BRI network and it is currently active.
Send *Pttn* Active, DLCI *nnnn*, *frame_relay_link*[1,3]	A selected Send Pattern test is active on the specified DLCI for the specified frame relay link.
Monitor *Pttn* Active, DLCI *nnnn*, *frame_relay_link*[1,3]	A selected Monitor Pattern test is active on the specified DLCI for the specified frame relay link.
Test Call Active, *ISDN Link Name*	A test call is active on the specified frame relay link, the link being the ISDN Link Name assigned in the ISDN Link Profile. This message would only appear for units with the ISDN DBM feature.

[1] *frame relay link* is one of the following:

- Net1-FR1. The frame relay link specified for the network interface, Network 1.
- Port-*n* for a 1-slot unit, or S*s*Port-*n* for a NAM in a multislot housing (the frame relay link associated with the specified user data port in the specified slot).
- *ISDN Link Name* on a non-network ISDN DBM interface.

[2] *Interface* is one of the following:

- Network 1
- DSX-1
- Port-*n*
- ISDN, BRI or PRI

[3] *nnnn* indicates a DLCI number of 16 through 1007.

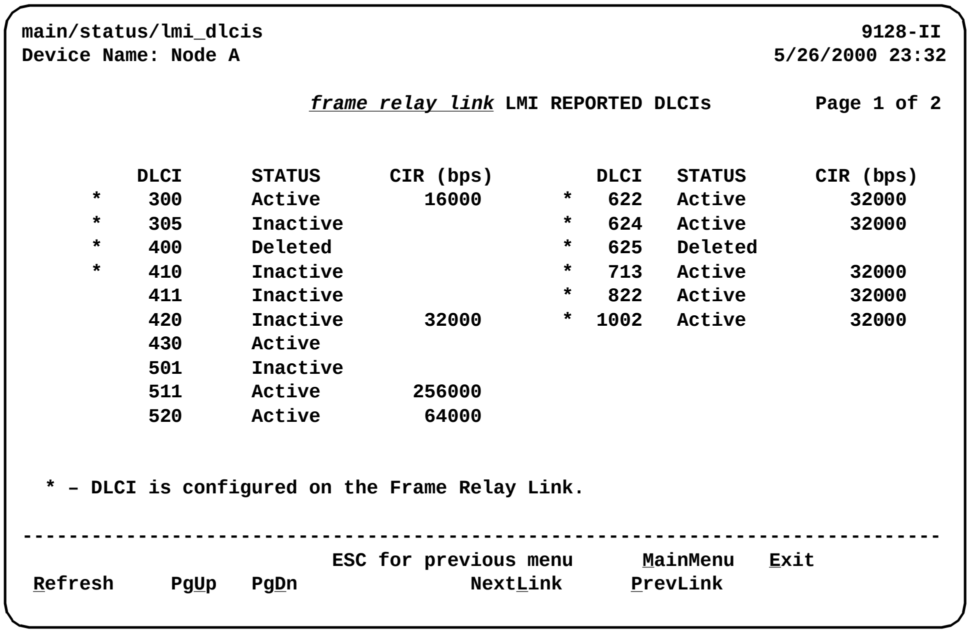
Network LMI-Reported DLCIs Status

Network LMI-reported DLCI statuses are selected from the Status menu.

Main Menu→Status→LMI Reported DLCIs

The LMI Reported DLCIs screen displays the status and CIR (if supported by the switch) for each DLCI, whether the DLCI is configured or not.

LMI-Reported DLCIs Status Screen Example



```
main/status/lmi_dlcis                                                    9128-II
Device Name: Node A                                               5/26/2000 23:32

                        frame relay link LMI REPORTED DLCIs         Page 1 of 2


          DLCI      STATUS      CIR (bps)        DLCI   STATUS      CIR (bps)
      *    300      Active        16000       *   622   Active         32000
      *    305      Inactive                  *   624   Active         32000
      *    400      Deleted                   *   625   Deleted
      *    410      Inactive                  *   713   Active         32000
           411      Inactive                  *   822   Active         32000
           420      Inactive      32000       *  1002   Active         32000
           430      Active
           501      Inactive
           511      Active       256000
           520      Active        64000


  * – DLCI is configured on the Frame Relay Link.

--------------------------------------------------------------------------------
                           ESC for previous menu      MainMenu   Exit
 Refresh     PgUp   PgDn               NextLink      PrevLink
```

An asterisk (*) next to the DLCI indicates that the DLCI has been configured for the link.

DLCIs without an asterisk have not been configured in the unit. These DLCIs pass through the unit transparently, without being monitored and with no demultiplexing/multiplexing of management diagnostics or user data being performed. Only DLCIs on the Net1-FR1 and Port-1 frame relay links appear on this screen; nonconfigured DLCIs on other links are discarded.

Table 7-10. Network LMI-Reported DLCIs Status

Field	Status	What It Indicates
DLCI	16 through 1007	Identifies the Local Management Interface-reported DLCI numbers assigned to the selected interface – the identifying number assigned to the path between two frame relay FrameSaver units' ports. DLCI statuses are listed in ascending order (i.e., lowest number first).
Status		LMI-reported status of the DLCI:
	Active	■ Whether the DLCI is active (capable of carrying data) in the frame relay network,
	Inactive	■ Whether it is inactive in the frame relay network,
	Deleted [1]	■ Whether it has been deleted by the frame relay network, or
	New[1]	■ Whether it has been created by the frame relay network.
CIR (bps)	0–1536000	Displays the committed information rate reported by the Stratacom switch. CIR information only appears in this column when LMI Protocol is set to Standard. If blank, the switch does not support this feature.

[1] Appears for 10 seconds only, before the network changes **`Deleted`** to **`Inactive`** and **`New`** to **`Active`**.

IP Path Connection Status

IP Path Connection Status is selected from the Status menu.

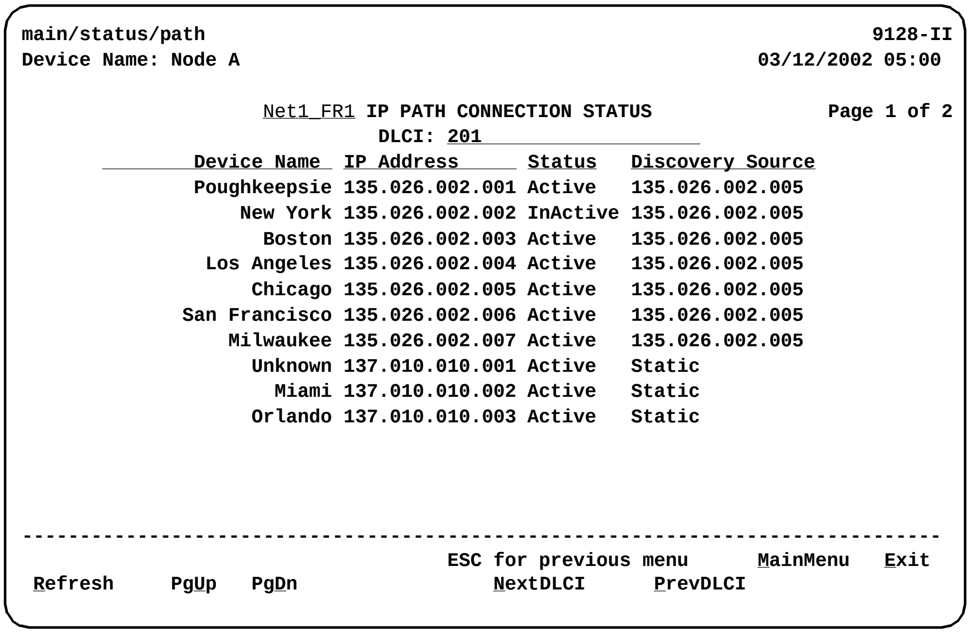
Main Menu→Status→IP Path Connection Status

The IP Path Connection Status screen displays the IP Path List, a list of devices that can be reached by their IP addresses for Service Level Management purposes.

The list is displayed in IP address order and includes both static addresses entered using the IP Path List (Static) configuration screen (see *Configuring the IP Path List* in Chapter 4, *Configuration Options*) and paths discovered as packets are received from other FrameSaver units

This screen only appears when Service Type is set to Frame Relay.

IP Path Connection Status Screen Example



```
main/status/path                                                          9128-II
Device Name: Node A                                             03/12/2002 05:00

                     Net1_FR1 IP PATH CONNECTION STATUS               Page 1 of 2
                               DLCI: 201
               Device Name  IP Address      Status   Discovery Source
               Poughkeepsie 135.026.002.001 Active   135.026.002.005
                   New York 135.026.002.002 InActive 135.026.002.005
                     Boston 135.026.002.003 Active   135.026.002.005
                Los Angeles 135.026.002.004 Active   135.026.002.005
                    Chicago 135.026.002.005 Active   135.026.002.005
              San Francisco 135.026.002.006 Active   135.026.002.005
                  Milwaukee 135.026.002.007 Active   135.026.002.005
                    Unknown 137.010.010.001 Active   Static
                      Miami 137.010.010.002 Active   Static
                    Orlando 137.010.010.003 Active   Static




--------------------------------------------------------------------------------
                                     ESC for previous menu      MainMenu   Exit
 Refresh     PgUp   PgDn                 NextDLCI      PrevDLCI
```

Table 7-11. IP Path Connection Status

Field	Status	What It Indicates
DLCI	16 through 1007	The IP Enabled DLCI.
Device Name	Up to 20 ASCII characters	The name of the device configured using the System Information screen of the Control branch, or Unknown if the device is not a FrameSaver.
IP Address	000.000.000.001 – 255.255.255.255	The IP address of the unit at the far end of the path.
Status		The status of the path:
	Active	■ The path is operational.
	Inactive	■ The path is not operational.
Discovery Source		The source of the path definition:
	■ Static	■ The path was entered using the IP Path List (Static) screen
	■ 000.000.000.001 – 255.255.255.255	■ This is the IP address of the FrameSaver unit that provided the path.

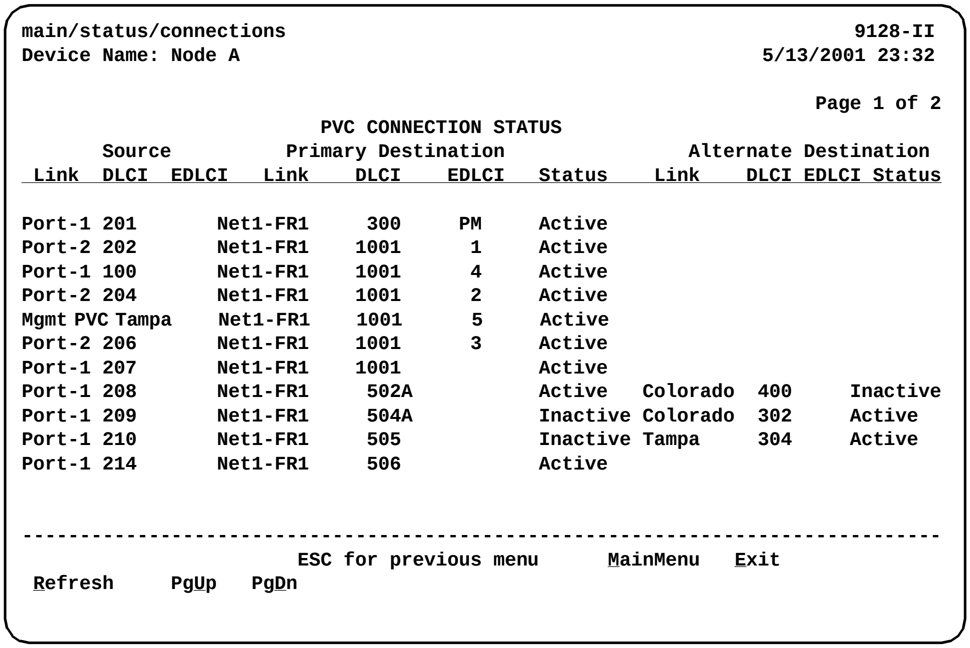
PVC Connection Status

PVC connection statuses are selected from the Status menu.

Main Menu→Status→PVC Connection Status

The PVC Connection Status screen shows all PVC connections and management links configured for the unit. The source and primary destination are shown, along with an alternate destination for backup. When a primary destination DLCI was assigned to a Backup Group, the Backup Group designation appears next to the DLCI number. In the example below, DLCIs 502 and 504 had been assigned to Backup Group A.

PVC Connection Status Screen Example



```
main/status/connections                                                  9128-II
Device Name: Node A                                              5/13/2001 23:32

                                                                     Page 1 of 2
                          PVC CONNECTION STATUS
       Source          Primary Destination                Alternate Destination
 Link  DLCI  EDLCI   Link    DLCI    EDLCI   Status    Link    DLCI EDLCI Status

Port-1 201       Net1-FR1     300     PM     Active
Port-2 202       Net1-FR1    1001      1     Active
Port-1 100       Net1-FR1    1001      4     Active
Port-2 204       Net1-FR1    1001      2     Active
Mgmt PVC Tampa   Net1-FR1    1001      5     Active
Port-2 206       Net1-FR1    1001      3     Active
Port-1 207       Net1-FR1    1001            Active
Port-1 208       Net1-FR1     502A           Active   Colorado  400     Inactive
Port-1 209       Net1-FR1     504A           Inactive Colorado  302     Active
Port-1 210       Net1-FR1     505            Inactive Tampa     304     Active
Port-1 214       Net1-FR1     506            Active


--------------------------------------------------------------------------------
                        ESC for previous menu      MainMenu   Exit
 Refresh     PgUp   PgDn
```

For units with ISDN backup capability, the DBM provides backup support through the unit's ISDN DBM interface. For units without ISDN backup capability, an alternate network DLCI can be used to backup user data. For additional information about the Alternate Destination fields, see *Configuring PVC Connections* in Chapter 4, *Configuration Options*.

If the **`No PVC Connections`** message appears instead of a list of PVC connections, no PVC connections have been configured yet.

Table 7-12. PVC Connection Status (1 of 2)

Field	Status	What It Indicates
Link	 Net1-FR1 Port-1, or Port-2 Mgmt*PVCName*	Identifies the cross-connection of DLCIs configured for the unit. ■ Source/destination is frame relay link 1 on Network 1 ■ User data port – Port-1, or Port-2 if a FrameSaver SLV 9128/9128-II ■ Virtual circuit is a management link that terminates in the unit, where *Name* is the link name
DLCI	16 to 1007	For standard DLCIs. Identifies an individual link/ connection embedded within a DLCI.
EDLCI	0 to 62 IP PM	For multiplexed DLCIs, a number from 0 to 62 identifies an individual link embedded within a DLCI. For IP Enabled DLCIs, IP is displayed. For payload managed DLCIs not IP Enabled, PM is displayed.

Table 7-12. PVC Connection Status (2 of 2)

Field	Status	What It Indicates
Status		Identifies whether the physical interfaces, LMIs, and DLCIs are all enabled and active for this PVC connection.
	Active *	■ The PVC is currently active.
	Inactive	■ The PVC is inactive because: – Alarm conditions and network and SLV communication status indicate that data cannot be successfully passed. – The unit has disabled the interface or frame relay link due to internal operating conventions. – Activation of an alternate virtual circuit is not warranted; that is, no alarm condition on the primary destination link has been detected.
	Disabled	■ The PVC cannot be activated and is essentially disabled as a result of how the unit was configured. Possible causes: – The physical interface at one or both ends of the PVC is/are disabled. – The frame relay link on one or both ends of the PVC is/are disabled.
	Invalid	■ Some portion of the PVC connection is not fully configured.

* For the circuit to be active, both Source and Destination Statuses must be Active.

Time Slot Assignment Status

Time slot assignments are made using the Time Slot Assignment configuration option. See *Assigning Time Slots/Cross Connections* in Chapter 4, *Configuration Options,* for making time slot assignments. Use the Timeslot Assignment Status screen to display time slot assignments for the network channels and the DSX-1 channels.

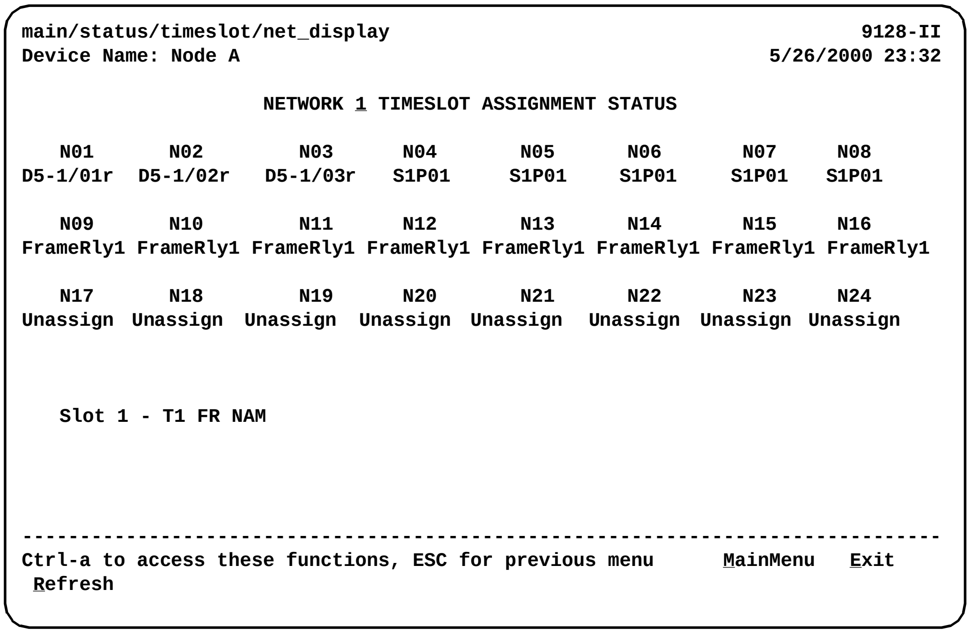
Displaying Network Time Slot Assignments

Use the Network Timeslot Assignment Status screen to display DS0 assignments for each DS0 on the network interface.

Main Menu→Status→Timeslot Assignment Status →Network

The Network Timeslot Assignment Status screen displays 24 two-field entries in three rows. Together, each two-field entry defines the assignment for one network interface time slot. The top field represents the timeslot of the network interface. The bottom field represents the cross-connect status of the associated (top field) network time slot.

Network Timeslot Assignment Status Screen Example



```
main/status/timeslot/net_display                                          9128-II
Device Name: Node A                                                5/26/2000 23:32

                     NETWORK 1 TIMESLOT ASSIGNMENT STATUS

   N01       N02        N03      N04       N05      N06       N07      N08
D5-1/01r  D5-1/02r  D5-1/03r   S1P01     S1P01    S1P01     S1P01    S1P01

   N09       N10        N11      N12       N13      N14       N15      N16
FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1

   N17       N18        N19      N20       N21      N22       N23      N24
Unassign  Unassign  Unassign  Unassign  Unassign  Unassign  Unassign  Unassign



   Slot 1 - T1 FR NAM





--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Refresh
```

The following information is available for network interface time slots (N01– N24).

The Cross Connect Status Field (bottom) . . .	Indicates . . .
Unassgn	The time slot is unassigned.
FrameRly1	The time slot is assigned to the network frame relay link.
Port-2	The synchronous data port (Port-2) is assigned to the network interface time slot (01 to 24).
D*s*-*p*/*tt*	The DSX-1 time slot *tt* is assigned to the network interface time slot (01 to 24).
D*s*-*p*/*tt*r	The DSX-1 time slot *tt* is assigned to the network interface time slot (01 to 24), using Robbed Bit Signaling (r).

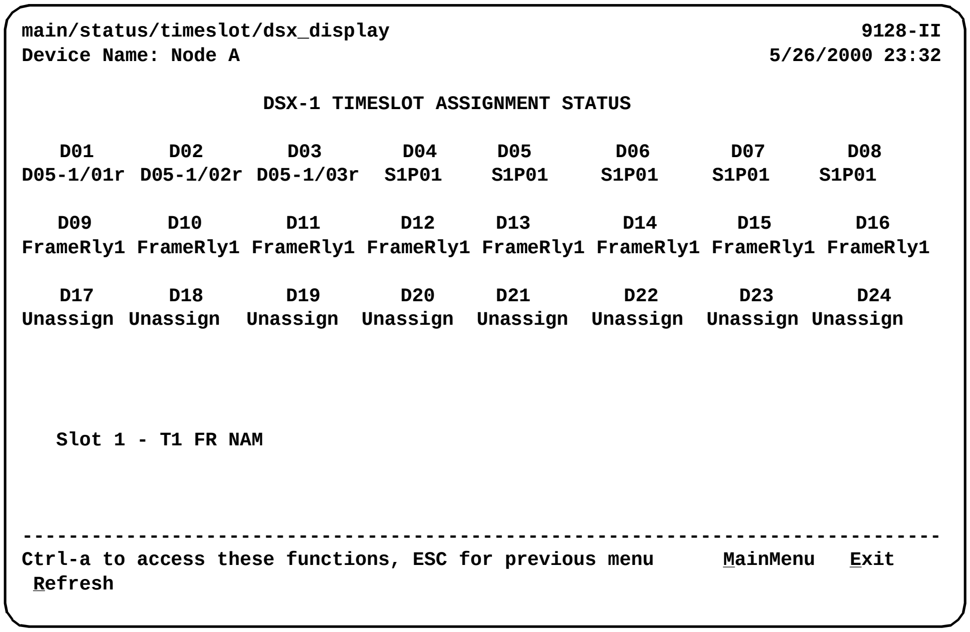
Displaying DSX-1 Time Slot Assignments

Use the DSX-1 Timeslot Assignments Status screen to display all of the DS0 assignments for each DS0 on the DSX-1 interface.

Main Menu→Status→Timeslot Assignment Status→DSX-1

The DSX-1 Timeslot Assignment Status screen displays 24 two-field entries in three rows. Together, each two-field entry defines the assignment for one DSX-1 interface time slot. The top field represents the time slot of the DSX-1 Interface. The bottom field represents the cross-connect status of the associated (top field) DSX-1 time slot.

DSX-1 Timeslot Assignment Status Screen Example



```
main/status/timeslot/dsx_display                                         9128-II
Device Name: Node A                                                5/26/2000 23:32

                     DSX-1 TIMESLOT ASSIGNMENT STATUS

   D01      D02        D03       D04     D05       D06       D07       D08
D05-1/01r  D05-1/02r  D05-1/03r  S1P01    S1P01     S1P01     S1P01     S1P01

   D09       D10       D11       D12     D13        D14       D15       D16
FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1 FrameRly1

   D17      D18        D19       D20     D21        D22       D23       D24
Unassign  Unassign  Unassign  Unassign  Unassign  Unassign  Unassign  Unassign




   Slot 1 - T1 FR NAM




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Refresh
```

The following information is available for DSX-1 interface time slots (D01– D24):

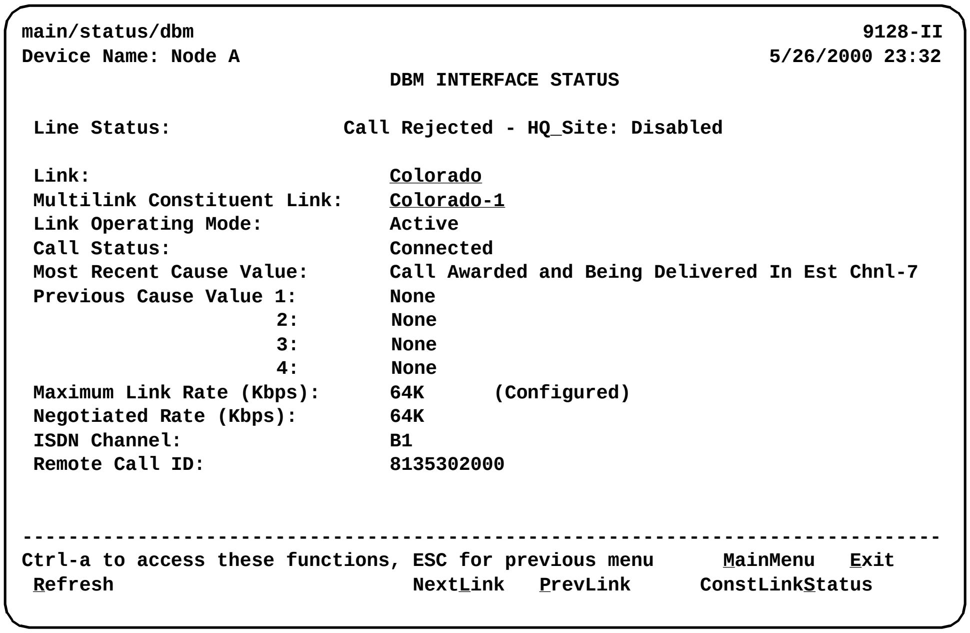
The Cross Connect Status Field (bottom) . . .	Indicates the . . .
blank	The time slot is unassigned.
Net1/*tt*	Network interface 1, time slot *(tt)* is assigned to DSX-1 time slot (01 to 24) using Clear Channel.
Net1/*tt*r	Network interface 1, time slot *(tt)* is assigned to DSX-1 time slot (01 to 24) using Robbed Bit Signaling (r).

DBM Interface Status

When an ISDN DBM is installed, these interface statuses appear when DBM Interface Status is selected from the Status menu.

Main Menu→Status→DBM Interface Status

DBM Interface Status Screen Example



```
main/status/dbm                                                          9128-II
Device Name: Node A                                                5/26/2000 23:32
                                DBM INTERFACE STATUS

 Line Status:              Call Rejected - HQ_Site: Disabled

 Link:                         Colorado
 Multilink Constituent Link:   Colorado-1
 Link Operating Mode:          Active
 Call Status:                  Connected
 Most Recent Cause Value:      Call Awarded and Being Delivered In Est Chnl-7
 Previous Cause Value 1:       None
                      2:       None
                      3:       None
                      4:       None
 Maximum Link Rate (Kbps):     64K      (Configured)
 Negotiated Rate (Kbps):       64K
 ISDN Channel:                 B1
 Remote Call ID:               8135302000


--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Refresh                         NextLink   PrevLink      ConstLinkStatus
```

Select the NextLink and PrevLink function keys to move forward or backward through the frame relay link that can be selected. If the selected frame relay link is a multilink aggregate link, select the ConstLinkStatus function key to see the status for selected constituent links.

For a multilink aggregate link, Multilink Constituent Link appears under Link so a specific constituent link can be selected. Otherwise, the line is blank. In addition, the Most Recent Cause Value, Previous Cause Values, and Remote Call ID do not appear for a multilink aggregate frame relay link.

Table 7-13. DBM Interface Status (1 of 3)

Field	Status	What It Indicates
Line Status		The overall status of the ISDN line.
	Active	■ The ISDN line is active and no error conditions exist.
	Disabled	■ The ISDN interface has been disabled. *Main Menu→ Configuration→ ISDN→ Physical*
	Inactive	■ The ISDN line is disconnected or an ISDN network alarm condition exists.
	Invalid SPID	■ The switch has rejected one of the configured SPIDs *(ISDN BRI DBM only)*.
	Invalid Local Number	■ The phone number configured for a B-channel is an invalid local number.
	Call Rejected – Invalid ID: *Caller ID*	■ The incoming call was rejected because the Caller ID or local phone number received from the switch did not match any configured Link Profiles. If provided by the switch, the rejected Caller ID is displayed after the status. Otherwise, **`Invalid Call ID`** is displayed.
	Call Rejected – No Far-End ID	■ The incoming call was rejected because no Caller ID was received from the switch (COM port's Port Use option is set to Caller ID). ■ No local phone number was received from the far-end device during the call validation process (COM port's Port Use option is set to Proprietary).
	Call Rejected – *ISDN Link Name:* Busy	■ The incoming call was rejected because the enabled ISDN Link Name associated with the incoming Caller1 ID or local phone number was busy. The ISDN Link Name associated with the incoming call is displayed.

[1] Only appears for a constituent frame relay link.

[2] If Link Operating Mode is Disabled or Idle, the Remote Call ID, ISDN Channel, and Negotiated Rate fields will not appear.

[3] Appears for frame relay links with only one constituent and for all constituent frame relay links.

Table 7-13. DBM Interface Status (2 of 3)

Field	Status	What It Indicates
Line Status *(continued)*	Call Rejected – *ISDN Link Name:* Disabled	■ The incoming call was rejected because the enabled ISDN Link Name associated with the incoming Caller1 ID or local phone number was disabled. The ISDN Link Name associated with the incoming call is displayed.
Link	*ISDN Link Name*	The selected ISDN backup link for which status will be displayed.
Multilink Constituent Link [1]	*ISDN Link Name*	The selected multilink constituent link for which status will be displayed.
Link Operating Mode		The status of the ISDN DBM.
	Disabled [2]	■ The ISDN Link Profile is disabled.
	Idle [2]	■ An ISDN link is not currently needed, so there is no ISDN connection.
	Active	■ The ISDN link is required for frame relay traffic and needs an active ISDN connection.
Call Status		The overall status of the ISDN frame relay link.
	Not Connected – Invalid Link Profile	■ No calls are currently connected on the selected link because the ISDN Link Profile is incomplete.
	Not Connected	■ No calls are currently connected on the selected link.
	Connected	■ At least one call is actively connected and available for data transfer on the selected ISDN frame relay link (when the Most Recent Cause Value is **`Call Awarded and Being Delivered In Est Chnl-7`**).
	Connected – Incoming Call [1]	■ An incoming call has been answered and is actively connected and available for data transfer on the selected multilink constituent link (when the Most Recent Cause Value is **`Call Awarded and Being Delivered In Est Chnl-7`**).

[1] Only appears for a constituent frame relay link.

[2] If Link Operating Mode is Disabled or Idle, the Remote Call ID, ISDN Channel, and Negotiated Rate fields will not appear.

[3] Appears for frame relay links with only one constituent and for all constituent frame relay links.

Table 7-13. DBM Interface Status (3 of 3)

Field	Status	What It Indicates
Call Status *(continued)*	Connected – Outbound Call[1]	■ An outbound call has been placed and is actively connected and available for data transfer on the selected multilink constituent link (when the Most Recent Cause Value is **`Call Awarded and Being Delivered In Est Chnl-7`**).
Most Recent Cause Value[3]	Various ITU cause messages	Refer to Table 7-14, Most Recent and Previous Cause Value Messages, for additional information.
Previous Cause Values[3]		
Maximum Link Rate (Kbps)	BRI DBM: 64K, 128K PRI DBM: 64K, 128K, . . . 1472	The maximum link rate that was configured for the selected link. This is the maximum rate the link will attempt to achieve when activated.
Negotiated Rate (Kbps)	64K per B-channel 56K per B-channel	The negotiated rate of the connection/link. For a multilink aggregate frame relay link, the negotiated rate will be the sum of the negotiated rates on all connected constituent links.
ISDN Channel	BRI DBM: B1, B2 PRI DBM: B1, B2, . . . B23	The ISDN B-channel being used for the call on this link.
Remote Call ID[3]	None	Backup has never been active on the link.
	Remote device's ID	Remote call origination – Last Calling ID of the remote backup device received for the B-channel. If the remote device initiated the call, this is the Inbound Call ID. If this device originated the call, this is the Outbound Phone Number.

[1] Only appears for a constituent frame relay link.

[2] If Link Operating Mode is Disabled or Idle, the Remote Call ID, ISDN Channel, and Negotiated Rate fields will not appear.

[3] Appears for frame relay links with only one constituent and for all constituent frame relay links.

Most Recent and Previous Cause Value Messages

The following Cause Value Messages are presented in alphabetical order. The Cause Number is also provided if you need to convert the message to its corresponding ITU number for your service provider.

Table 7-14. Most Recent and Previous Cause Value Messages (1 of 6)

Message	Cause No.	What It Indicates	What To Do
Bearer Capability Not Authorized	57	User has requested a bearer capability that the user is not authorized to use.	Arrange for the desired capability.
Bearer Capability not Implemented	65	Device sending this cause does not support the bearer capability (i.e., channel type) requested.	Arrange for the desired capability.
Bearer Capability Presently Not Available	58	Bearer capability requested is supported by the device generating the cause, but it is not available at this time.	Arrange for the desired capability.
Call Awarded and Being Delivered in Est Chnl-7	7	An incoming call is being connected to an already established channel that is used for similar calls.	No action is needed.
Call Rejected	21	Equipment sending the cause does not want to receive the call at this time.	No action is needed.
Call Terminated by Remote End	130	Remote DBM rejected or terminated the call.	1. Retry the call. 2. Verify that the remote DBM's link profile is correct.
Call With Requested Call ID Has Been Cleared	86	Network has received a call resume request, but the call had been cleared after it was suspended.	No action is needed.
Channel Type Not Implemented	66	Device sending this cause does not support the requested channel type.	Arrange for the desired capability.
Channel Unacceptable	6	Channel identified for the call is not acceptable to the receiving device.	Arrange for the desired capability.
Destination Out of Order	27	Destination interface specified is not functioning correctly so the signalling message could not be delivered (e.g., physical or data-link layer failure at the remote end, user equipment is offline).	Verify that the remote DBM's link profile is correct.

Table 7-14. Most Recent and Previous Cause Value Messages (2 of 6)

Message	Cause No.	What It Indicates	What To Do
Facility Rejected	29	Requested facility is not provided by the network.	No action is needed.
Incoming Calls Barred	54	Called user is not permitted to accept the call.	Turn off network call screening.
Incompatible Destination	88	Request to establish a call has been received, but low-layer, high-layer, or another compatibility attribute (e.g., data rate) cannot be provided. Incorrect format of the destination link.	Arrange for the desired capability.
Identified Channel Does Not Exist	82	Channel requested for a call is not activated on the interface.	Make sure the network is configured for 2B service, if a BRI DBM. Contact your service provider to verify that your service is provisioned for two B-channels.
Info Element Nonexistent or Nonimplemented	99	Device sending this cause has received a message it does not recognize. This cause will not prevent the message from being precessed.	1. Verify that the Inbound Calling ID has been defined. 2. Verify that the Inbound Calling ID is part of your service.
Interworking, Unspecified	127	Precise cause of a message cannot be determined because the interworking network does not provide causes.	No action is needed.
Invalid Call Reference Value	81	Call reference used is not currently in use on the user-network interface.	Contact your service representative.
Invalid Info Element Contents	100	Device sending this cause has received and implemented an information element, but one or more fields in the element cannot be processed.	Contact your service representative.
Invalid Message, Unspecified	95	No other cause in the invalid message class applies for this invalid message event.	Contact your service representative.
Invalid Number Format – Incomplete Address	28	Call cannot be completed because the phone number is incorrect or incomplete.	Check your ISDN link profile, and correct the number.

Table 7-14. Most Recent and Previous Cause Value Messages (3 of 6)

Message	Cause No.	What It Indicates	What To Do
Invalid Transit Network Selection	91	Incorrect format of transit network identification.	Contact your service representative.
Mandatory Information Element Missing	96	Required data is missing from a mandatory information element.	Contact your service representative.
Message Not Compatible with Call State	101	Device sending this cause has received a message that is not permissible while in the call state.	Contact your service representative.
Msg Nonexistent	98	An unexpected message was received in a state other than Null.	Retry the call.
Msg Type Nonexistent or Unimplemented	97	Device sending this cause has received a nonexistent or not implemented message type while in the call state. Device sending this cause has received a status message that indicates an incompatible call state.	Contact your service representative.
Network Out of Order	38	Network is not functioning correctly, and the condition is expected to continue.	Contact your service representative.
No Call Suspended	85	A call resume has been issued, but no calls have been suspended.	No action is needed.
No Circuit/Channel Available	34	No circuit/channel is currently available to handle the call.	Wait and try again.
No Destination Route	3	Network through which call has been routed does not serve the destination area or device.	Contact your service representative.
None	—	No causes have been generated.	No action is needed.
Non-selected User Clearing	26	User has not been awarded the incoming call.	No action is needed.
No Route to Specify Transit Network	2	The device sending or receiving this cause does not recognize the transit network that the call is being/has been routed through.	1. Verify that the network exists. 2. Verify that the network serves the device sending the cause.

Table 7-14. Most Recent and Previous Cause Value Messages (4 of 6)

Message	Cause No.	What It Indicates	What To Do
Normal Call Clearing	16	Call is being cleared because either the caller or receiver has requested that it be cleared.	No action is needed.
Normal, Unspecified	31	Remote user has sent a release message to the network. No other cause in the normal class applies for this normal event.	No action is needed.
No User Responding	18	Called device does not respond to the call with an alert or connect indication within the prescribed period of time. Internal network timers may be a cause.	Contact the network provider if the cause continues.
Number Changed	22	Called number is no longer assigned.	Look in the diagnostic field for the new number, then change the phone number in your ISDN link profile.
Only Restricted Bearer Capability Available	70	An unrestricted bearer service has been requested, but the device sending the cause only supports the restricted version.	Arrange for the desired capability.
Outgoing Calls Barred	52	Network is using Call Screening.	Contact the network provider to turn Call Screening off.
Pre-empted	45	Call has been pre-empted.	Contact the network provider.
Protocol Error, Unspecified	111	No other cause in the protocol error class applies for this protocol error event.	Contact your service representative.
Quality of Service Unavailable	49	Requested Quality of Service requested cannot be provided (e.g., throughput cannot be supported).	No action is needed.
Recovery of Timer Expired	102	Error-handling procedure has been initiated as a result of the expiration of a timer.	Retry the call.

Table 7-14. Most Recent and Previous Cause Value Messages (5 of 6)

Message	Cause No.	What It Indicates	What To Do
Requested Channel Not Available	44	Circuit or channel requested cannot be provided by the other side of the interface.	Allow the DBM to automatically call using the alternate link if Auto Backup is enabled, or manually select an alternate path for the call.
Requested Facility Not Implemented	69	Supplemental service requested is not supported by this device.	No action is needed.
Requested Facility Not Subscribed	50	The supplementary service requested cannot be provided by the network until user completes arrangement with its supporting networks.	Arrange for the desired capability.
Resource Unavailable, Unspecified	47	No other cause in the resource unavailable class applies for this resource unavailable event.	No action is needed.
Response to STATus ENQuiry	30	Status enquiry message received, generating this message.	No action is needed.
Service/Option Not Implemented	79	No other cause in the service or option not available class applies for this not implemented event.	No action is needed.
Service/Option Unavailable, Unspecified	63	No other cause in the service or option not available class applies for this not available event.	Wait and try again.
Switching Equipment Congestion	42	Switching equipment sending the cause is experiencing heavy traffic.	Wait and try again.
Suspended Call Exists, But Not Call ID	83	A call resume has been attempted, but no suspended call exists for this phone number.	1. Verify the number in the Inbound Calling ID # field for the suspended call. 2. Reissue the Call Resume command using the correct number.
Temporary Failure	41	Network is not functioning correctly, but the condition is not expected to continue for long.	Wait and try again.

Table 7-14. Most Recent and Previous Cause Value Messages (6 of 6)

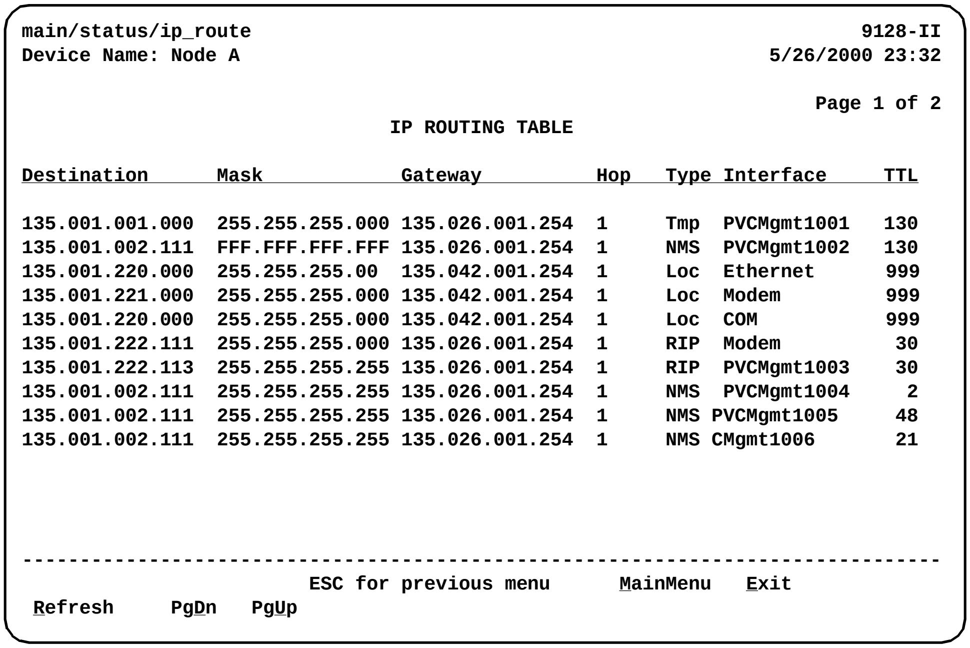
Message	Cause No.	What It Indicates	What To Do
Unallocated Number	1	Destination requested cannot be reached because the Inbound Calling ID number is not assigned or allocated.	Assign the Inbound Calling ID.
User Access Information Discarded	43	Network was unable to deliver the access information when trying to establish the call.	No action is needed.
User Alerting, No Answer	19	During call establishment, an alerting was received but a connection was not.	1. Verify that the remote device is operational and configured to answer. 2. Retry the call.
User Busy	17	Called number cannot receive the call.	Wait and try again.

IP Routing Table

The IP Routing Table shows all the routes configured in the FrameSaver unit.

Main Menu→Status→IP Routing Table

IP Routing Table Screen Example



```
main/status/ip_route                                                     9128-II
Device Name: Node A                                              5/26/2000 23:32

                                                                     Page 1 of 2
                                IP ROUTING TABLE

Destination      Mask            Gateway          Hop   Type Interface     TTL

135.001.001.000  255.255.255.000 135.026.001.254  1     Tmp  PVCMgmt1001   130
135.001.002.111  FFF.FFF.FFF.FFF 135.026.001.254  1     NMS  PVCMgmt1002   130
135.001.220.000  255.255.255.00  135.042.001.254  1     Loc  Ethernet      999
135.001.221.000  255.255.255.000 135.042.001.254  1     Loc  Modem         999
135.001.220.000  255.255.255.000 135.042.001.254  1     Loc  COM           999
135.001.222.111  255.255.255.000 135.026.001.254  1     RIP  Modem          30
135.001.222.113  255.255.255.255 135.026.001.254  1     RIP  PVCMgmt1003    30
135.001.002.111  255.255.255.255 135.026.001.254  1     NMS  PVCMgmt1004     2
135.001.002.111  255.255.255.255 135.026.001.254  1     NMS PVCMgmt1005     48
135.001.002.111  255.255.255.255 135.026.001.254  1     NMS CMgmt1006       21




--------------------------------------------------------------------------------
                         ESC for previous menu      MainMenu   Exit
 Refresh     PgDn   PgUp
```

The table is sorted by the Destination IP address, from the lowest number to the highest. If no routes exist, the **No Routes** message appears instead of routing information.

Table 7-15.   IP Routing Table Values (1 of 2)

Column	What It Indicates
Destination	The Destination IP Address for the route: 001.000.000.000 – 223.255.255.255
Mask	The Destination Subnet Mask for the route: ■ 000.000.000.000 – 255.255.255.255 for network routes ■ FFF.FFF.FFF.FFF for host routes ■ 127 may appear as well. It is a reserved number.
Gateway	The Gateway IP Address for the route: 001.000.000.000 – 223.255.255.255
Hop	The number of hops in the route to the destination (1–15). If 16 appears, the route is in the process of being aged out.

Table 7-15. IP Routing Table Values (2 of 2)

Column	What It Indicates
Type	The method used to add the route to the table. ■ RIP: The route was discovered through Routing Information Protocol. The route remains until its TTL (Time to Live) expires, a better route is provided via RIP, or there is a power reset. ■ Loc: The route was added due to the FrameSaver unit's local configuration; a Default IP Address or an SNMP Manager Initial Route Destination have been configured. The route remains until the unit's configuration changes. ■ NMS: The route was added by a Network Management System using SNMP (Simple Network Management Protocol). The route remains until there is a power reset of the unit. ■ ICMP: The route was added because an ICMP (Internet Control Management Protocol) redirect message was received from a router indicating a better route to the destination. That is, a datagram was sent to a router and the router is informing the datagram source through an ICMP redirect message of a better route. ■ Tmp: The route was added as a temporary route in order to respond to an IP packet that was received. The route remains until its TTL expires or there is a power reset.
Interface	Specifies the interface to be used to reach the destination. ■ COM: Communications port ■ PVC*name*: Name of the management PVC (e.g., PVCMgmt1001) ■ Internal: The interface to be used for software loopbacks or internal device functions in order to reach the destination.
TTL	The Time to Live that was set for the route, in seconds: 1 – 999. If 999 appears, the route is a permanent one.

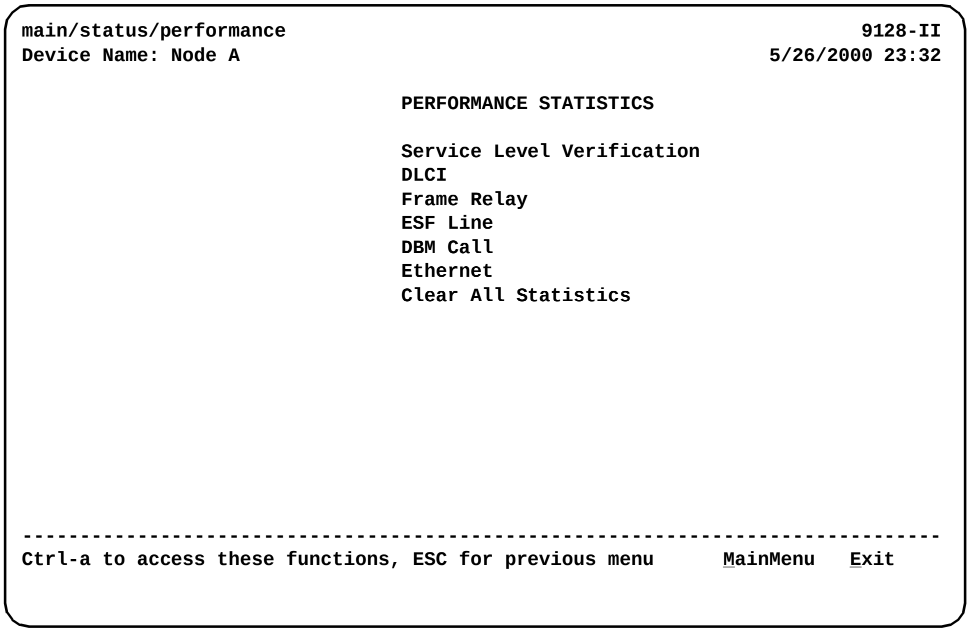
Performance Statistics

Use the Performance Statistics menu to display statistical information for a selected interface. Statistical information is useful when trying to determine the severity and frequency or duration of a condition.

Main Menu→Status→Performance Statistics

Physical and link layer statistics (Layers 1 and 2) are collected on the port. The following menu shows the performance statistics that can be selected.

Performance Statistics Menu



```
main/status/performance                                                 9128-II
Device Name: Node A                                                 5/26/2000 23:32

                                 PERFORMANCE STATISTICS

                                 Service Level Verification
                                 DLCI
                                 Frame Relay
                                 ESF Line
                                 DBM Call
                                 Ethernet
                                 Clear All Statistics









--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

DBM Call Statistics only appear when the FrameSaver unit has the ISDN DBM feature, and Ethernet only appears for the FrameSaver SLV 9126-II or 9128-II.

Clearing Performance Statistics

Performance statistics counters can be reset to the baseline when using a directly-connected asynchronous terminal and your security Access Level is Level-1. This feature is useful when troubleshooting problems.

Statistic counters are not actually cleared using this feature. True statistic counts are always maintained so SLAs can be verified, and they can be viewed from an SNMP NMS. However, since statistics can be cleared locally, the statistics viewed via the menu-driven user interface may be different from those viewed from the NMS.

▶ Procedure

To clear all statistics:

Performance Statistics → Clear All Statistics

▶ Procedure

To clear specific sets of statistics:

- Use the ClrSLV&DLCIStats function key to reset the SLV and DLCI performance statistic counters for the currently displayed DLCI from one of the following screens:

  Performance Statistics → Service Level Verification
  Performance Statistics → DLCI

- Use the ClrLinkStats function key to reset the frame relay link performance statistics.

  Performance Statistics → Frame Relay

- Use the ClrNearStats or ClrFarStats function key to reset all near-end or all far-end Extended SuperFrame (ESF) line performance statistics.

  Performance Statistics → ESF Line

- Use the ClrDBMStats function key to reset the DBM call performance statistics.

  Performance Statistics → DBM Call

- Use the ClrStats function key to reset all Ethernet port performance statistics.

  Performance Statistics → Ethernet

Service Level Verification Performance Statistics

These statistics appear when Service Level Verification (SLV) is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics→ Service Level Verification

They only appear for the network interface and only if DLCIs are multiplexed or IP Enabled.

Information displayed on the SLV Performance Statistics screen depends on DLCI type. See Table 7-16, SLV Performance Statistics for Multiplexed DLCI or Table 7-17, SLV Performance Statistics for IP Enabled DLCI.

On either screen, select PrevDLCI or NextDLCI to view statistics for the previous or next DLCI on the link. On the IP Enabled DLCI screen, select PrevPath or NextPath to view statistics for the previous or next path associated with the DLCI.

For standard or multiplexed DLCIs, the statistics collected by the unit depend upon the device at the far end of the connection. If the far-end device is a FrameSaver SLV unit, frame relay, latency, and FDR/DDR performance statistics are collected. The Frame Relay Delivery Ratio is the number of delivered frames/offered frames; the Data Delivery Ratio is the number of delivered octets/offered octets.

If the far-end device is a non-FrameSaver device, or a FrameSaver 9120 or 9620, only frame relay statistics are collected.

Table 7-16. SLV Performance Statistics for Multiplexed DLCI (1 of 3)

Statistic	What It Indicates
Far End Circuit	Number of the multiplexed DLCI or VPI/VCI (Virtual Path Identifier/Virtual Channel Identifier) at the other end of the connection. If the far-end circuit is a DLCI, the DLCI number (16–1007) appears. If a VPI/VCI, the number is displayed as *xx,yyy,* xx being the VPI number (0–15) and *yyy* being the VCI number (32–2047). **None** appears if the unit has not communicated with the other end.
Far End IP Addr	IP Address of the device at the other end of the multiplexed DLCI connection. **None** appears if the FrameSaver unit has not communicated with the other end, or if the device at the other end of the multiplexed DLCI does not have an IP Address configured.
Dropped SLV Responses	The number of SLV inband sample messages sent for which a response from the far-end device has not been received.

* Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.

Table 7-16.   SLV Performance Statistics for Multiplexed DLCI (2 of 3)

Statistic	What It Indicates
Inbound Dropped Frames*	Total number of frames transmitted by the far-end device that were dropped in transit. The counts continue to increment until the maximum value is reached (2^{32}–2), then the count starts over. The SLV Delivery Ratio option (see Table 4-4, Service Level Verification Options, in Chapter 4, *Configuration Options*,) must be enabled for these statistics to appear.
■ Above CIR*	■ The number of frames transmitted by the far-end device that were above the committed information rate and were dropped in transit.
■ Within CIR*	■ The number of frames transmitted by the far-end device that were within the committed information rate, but were dropped in transit.
■ Between CIR&EIR*	■ The number of frames transmitted by the far-end device that were between the committed information rate and excess information rate, and were dropped in transit.
■ Above EIR*	■ The number of frames transmitted by the far-end device that were above the excess information rate and were dropped in transit.
Inbound Dropped Characters*	Total number of bytes transmitted by the far-end device that were dropped in transit. The counts continue to increment until the maximum value is reached (2^{32}–2), then the count starts over. The SLV Delivery Ratio option (see Table 4-4, Service Level Verification Options, in Chapter 4, *Configuration Options*,) must be enabled for these statistics to appear. **NA** appears instead of a statistical count if FDR/DDR (Frame Delivery Ratio/Data Delivery Ratio) information is not being received from the far-end device.
■ Above CIR*	■ The number of bytes transmitted by the far-end device that were above the committed information rate and were dropped in transit.
■ Within CIR*	■ The number of bytes transmitted by the far-end device that were within the committed information rate, but were dropped in transit.
■ Between CIR&EIR*	■ The number of bytes transmitted by the far-end device that were between the committed information rate and excess information rate, and were dropped in transit.
■ Above EIR*	■ The number of bytes transmitted by the far-end device that were above the excess information rate and were dropped in transit.

* Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.

Table 7-16. SLV Performance Statistics for Multiplexed DLCI (3 of 3)

Statistic	What It Indicates
Latest RdTrip Latency	Current round trip latency, measured in milliseconds, between the FrameSaver unit and the device at the other end of the multiplexed DLCI connection. "--" appears if communication with the far-end device is not successful.
Avg RdTrip Latency	Average round trip latency, measured in milliseconds, between the FrameSaver unit and the device at the other end of the multiplexed DLCI connection. Average round trip latency is measured every SLV sampling interval and the average is computed (using packets with the configured SLV Packet Size (bytes), Table 4-4, Service Level Verification Options, in Chapter 4, *Configuration Options*,) over the previous 15 samples. If SLV Packet Size is changed, a new average is not available until a new sample has been received. "--" appears if communication with the far-end device over the last 15 samples has not been successful.
Max RdTrip Latency	Same as average (Avg RdTrip Latency), but storing the maximum value of latency over the previous 15 samples. "--" appears if communication with the far-end device over the last 15 samples has not been successful.

* Only appears for FrameSaver units when the SLV Delivery Ratio option is enabled.

For an IP Enabled DLCI, statistics are shown for last, minimum, average, and maximum round trips, and for dropped SLV responses, for each of the seven classes of service.

Table 7-17. SLV Performance Statistics for IP Enabled DLCI (1 of 2)

Statistic	What It Indicates
Far End IP Addr	IP Address of the device at the other end of the DLCI connection. **None** appears if the FrameSaver unit has not communicated with the other end, or if the device at the other end of the DLCI does not have an IP Address configured.
Path Up Time	The number of days, hours, minutes, and seconds since the last transition of this DLCI from Inactive to Active.
Far End Circuit	Number of the DLCI at the other end of the connection. **None** appears if the unit has not communicated with the other end.
SLM Poll Type	The role played by the far-end FrameSaver in the collection of latency and availability statistics. **Initiator** – The far-end FrameSaver initiates the SLV packet used for statistics collection. **Responder** – The far-end FrameSaver returns the SLV packet sent by the Initiator.
Far End Name	The system name configured for the far-end FrameSaver device, obtained using its IP address. **Unknown** appears if the far end device is not a FrameSaver or if no response has been received since the last reset.
COS Type Mismatches	The number of SLV packets received that indicate a mismatch between the Class of Service definitions in the near-end and far-end devices.
Far End Type	The model type of the far-end FrameSaver device, obtained using its IP address. **Unknown** appears if the far end device is not a FrameSaver or if no response has been received since the last reset.
COS Name	The names for different Classes of Service defined using the Class of Service Definitions screen. See *Configuring Class of Service Definitions* in Chapter 4, *Configuration Options*.
COS ID	The ID numbers (1–7) of the Class of Service definitions.
Last RdTrip	Current round trip latency, measured in milliseconds, between the FrameSaver unit and the device at the other end of the DLCI connection. **Unknown** appears if communication with the far-end device is not successful.
Min RdTrip	Minimum round trip latency measured over the last 15 samples between the FrameSaver unit and the device at the other end of the DLCI connection. **"--"** appears if communication with the far-end device over the last 15 samples has not been successful.

Table 7-17. SLV Performance Statistics for IP Enabled DLCI (2 of 2)

Statistic	What It Indicates
Avg RdTrip	Average round trip latency between the FrameSaver unit and the device at the other end of the DLCI connection. Average round trip latency is measured every SLV sampling interval and the average is computed (using packets with the configured SLV Packet Size (bytes), Table 4-4, Service Level Verification Options) over the previous 15 samples. If SLV Packet Size is changed, a new average is not available until a new sample has been received. "--" appears if communication with the far-end device over the last 15 samples has not been successful.
Max RdTrip	Same as average (Avg RdTrip), but storing the maximum value of latency over the previous 15 samples. "--" appears if communication with the far-end device over the last 15 samples has not been successful.
Dropped SLV Responses	The number of SLV inband sample messages sent for which no response from the far-end device has been received.

DLCI Performance Statistics

These statistics appear when DLCI is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics→ DLCI

Table 7-18. DLCI Performance Statistics (1 of 2)

Statistic	What It Indicates
DLCI Up Since *	Date and time that the DLCI was last declared Active after a period of inactivity. Down is displayed if the DLCI is inactive. If the DLCI was Down, this is the time that the DLCI recovered. If the DLCI was never Down, this is the first time the unit discovered that the DLCI was active in the network.
DLCI Up Time *	Days, hours, minutes, and seconds since the DLCI was last declared Active after a period of inactivity. Down is displayed if the DLCI is inactive. If the DLCI was Down, this is the amount of time since the DLCI recovered. If the DLCI was never Down, this is the amount of time since the unit discovered that the DLCI was active in the network.
Total Tx Frames/ Tx Octets	Total number of data frames and octets (8-bit bytes) transmitted for the selected DLCI on the frame relay link.
■ Within CIR	■ The number of frames and octets sent by the far-end device for on the selected DLCI of the frame relay link that were within the committed information rate.
■ Between CIR&EIR	■ The number of frames and octets sent by the far-end device on the selected DLCI of the frame relay link that were between the committed information rate and excess information rate.
■ Above EIR	■ The number of frames and octets sent by the far-end device on the selected DLCI of the frame relay link that were above the excess information rate.
■ With DE Set	■ The number of frames and octets sent on the selected DLCI of the frame relay link with the discard eligible bit set.
■ With BECN Set	■ The number of frames and octets sent on the selected DLCI of the frame relay link with backward explicit congestion notifications. BECNs are sent to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.

* Only appears for the network interface.

Table 7-18. DLCI Performance Statistics (2 of 2)

Statistic	What It Indicates
Total Rx Frames/ Rx Octets	Total number of data frames and octets (8-bit bytes) received for the selected DLCI on the frame relay link.
■ Within CIR	■ The number of frames and octets received on the selected DLCI of the frame relay link that were within the committed information rate.
■ Between CIR&EIR	■ The number of frames and octets received on the selected DLCI of the frame relay link that were between the committed information rate and excess information rate.
■ Above EIR	■ The number of frames and octets received on the selected DLCI of the frame relay link that were above the excess information rate.
■ With DE Set	■ The number of frames and octets received on the selected DLCI of the frame relay link with the discard eligible bit set.
■ With BECN Set	■ The number of frames and octets received on the selected DLCI of the frame relay link with backward explicit congestion notifications. BECNs are sent to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.
■ With FECN Set	■ The number of frames and octets received on the selected DLCI of the frame relay link with forward explicit congestion notifications. The network sends FECNs to notify users of data traffic congestion in the same direction of the frame carrying the FECN indicator.

* Only appears for the network interface.

Additional Performance Statistics for IP Enabled DLCI

If the selected DLCI is IP Enabled, the DLCI Performance Statistics screen has a second page listing statistics by Class of Service. On the first DLCI Performance Statistics page for an IP Enabled DLCI, PgUp and PgDn are shown as available commands in the function keys area of the screen. Select PgUp or PgDn to display the second page.

Table 7-19. Additional Performance Statistics for IP Enabled DLCI

Statistic	What It Indicates
Class of Svc Name	The names for different Classes of Service defined using the Class of Service Definitions screen. See *Configuring Class of Service Definitions* in Chapter 4, *Configuration Options*.
Class of Svc ID	The ID numbers (1–7) of the Class of Service definitions.
The following IP statistics are shown for: ■ The seven Classes of Service ■ **Unknown COS** – IP packets whose Type of Service values do not match those defined for any Class of Service ■ **Non-IP** – Packets that were not IP Version 4 ■ **Total** – The total for all packets	
Tx Packets	The number of packets transmitted
Tx Octets	The number of octets in the packets transmitted
Rx Packets	The number of packets received
Rx Octets	The number of octets in the packets received
Rx Errors	The number of packets received in error

Frame Relay Performance Statistics

The following statistics appear when Frame Relay is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → Frame Relay

All counts continue to increment until the maximum value is reached (2^{32}–2), then the count starts over. The NextLink and PrevLink function keys only appear when multiple frame relay links have been configured.

For FrameSaver units with an ISDN DBM:

All enabled multilink aggregate links are available for selection from the Frame Relay Performance Statistics screen. The multilink aggregate link must be enabled if statistics are to be collected for this frame relay link. When the frame relay link is the multilink aggregate link, statistics for its related constituent links can be viewed.

To view the statistics for a multilink constituent link, select the ConstLinkStats function key. All enabled multilink constituent links become available for selection. Select the desired constituent link from the Multilink Constituent Link field.

The frame relay performance statistics collected for any frame relay link are collected for multilink frame relay links, unless the link is a multilink aggregate link. In this case, statistics for Frame Relay LMI and Frame Relay HDLC Errors are not collected; these statistics are available for multilink constituent links only.

Table 7-20. Frame Relay Performance Statistics (1 of 4)

Statistic	What It Indicates
Frame Relay Link	
Frames Sent	The number of frames sent over the interface.
Frames Received	The number of frames received over the interface.
Characters Sent	The number of data octets (bytes) sent over the interface.
Characters Received	The number of data octets (bytes) received over the interface.
FECNs Received	The number of forward explicit congestion notifications received over the interface. The network sends FECNs to notify users of data traffic congestion in the same direction of the frame carrying the FECN indicator.
BECNs Received	The number of backward explicit congestion notifications received over the interface. The network sends BECNs to notify users of data traffic congestion in the opposite direction of the frame carrying the BECN indicator.

Table 7-20. Frame Relay Performance Statistics (2 of 4)

Statistic	What It Indicates
Frame Relay Errors	
Total Errors	The number of total frame relay errors, excluding LMI errors. Short frames, long frames, invalid DLCIs, unknown DLCIs, and unknown errors are included in this total. Indicates that there may be a non-frame relay device on the other end of the link, or the units at either the far end or both ends of the link may be configured incorrectly.
Invalid Rx Frames	The number of invalid frames received over the Network or Port-1 interface. There is a non-frame relay device on the other end of the link.
Short Rx Frames	The number of frames received over the Network or Port-1 interface that were less than 5-octets (five 8-bit bytes) in length. There may be a non-frame relay device on the other end of the link.
Long Rx Frames	The number of frames received over the Network or Port-1 interface that were more than 8192-octets in length. The device on the far end of the link may be configured incorrectly.
Invalid DLCI	The number of frames received over the interface that were addressed to DLCIs outside the valid range; that is, a number less than 16 or greater than 1007. The device on the far end of the circuit may have been configured incorrectly, or the DLCIs configured for the FrameSaver unit may not match the DLCIs supplied by the service provider.
Unknown DLCI	The number of frames received over the interface that were addressed to unknown DLCIs. The DLCI may not have been configured, or it has been configured to be Inactive. Indicates that the FrameSaver units or devices at both or either end of the circuit have been configured incorrectly.
Unknown Error	The number of frames received over the interface that do not fall into one of the other statistic categories. Indicates that the error is not one that the unit can recognize.

Table 7-20. Frame Relay Performance Statistics (3 of 4)

Statistic	What It Indicates
Frame Relay LMI	
LMI Protocol	The LMI protocol configured for the frame relay link. Normal condition.
Status Msg Received	The number of LMI status messages received over the interface. Normal condition.
Total LMI Errors	The number of LMI errors. Reliability errors, protocol errors, unknown report types, unknown information elements, and sequence errors are included in this total. Network problems.
Number of Inactives	The number of times the LMI has declared the frame relay link Inactive. Network problems.

Table 7-20. Frame Relay Performance Statistics (4 of 4)

Statistic	What It Indicates
Frame Relay HDLC Errors	
Rx Total Errors	The number of receiver errors on the interface. The following are included in this count: ■ Receive invalid frames (short frames, long frames, invalid DLCIs, unknown DLCIs, and unknown errors) ■ Rx Total Discards ■ Receive errors (non-octet aligned frames, frames with CRC errors, and Rx Overruns)
Rx Total Discards	The number of receiver discards on the interface. The following are included in this count: ■ Resource errors ■ Rx Overruns ■ Frames received when the link was down ■ Inactive and disconnected DLCIs ■ Inactive destination DLCIs ■ Unknown EDLCIs
Rx Overruns	The number of receiver overruns (too many bits) on the interface.
Rx Non-Octet Frames	The number of non-octet frames received on the interface.
Rx CRC Errors	The number of received CRC (cycle redundancy check) errors.
Tx Total Errors	The total number of transmit errors on the interface, including transmits discards and transmit overruns.
Tx Total Discards	The total number of transmit discards on the interface, including underrun flushes.
Tx Underruns	The number of transmitter underruns (too few bits) on the interface.

ESF Line Performance Statistics

These statistics appear when ESF Line is selected from the Performance Statistics menu for the network interface.

Main Menu → Status → Performance Statistics → ESF Line

Only seven T1 network statistical intervals appear on the screen at any one time. You can choose which intervals to display on your screen by entering:

- Interval Number (01–96)

  – or –

- Time (Hours and Minutes)

NOTES:

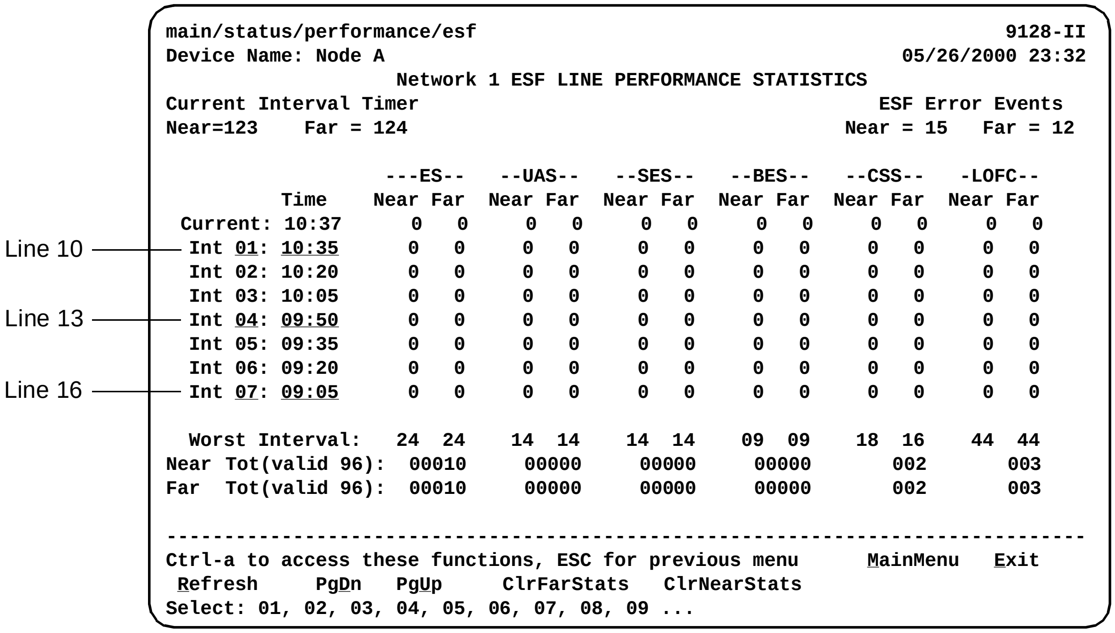
— Interval 01 is the interval occurring just prior to the current one;
Interval 02 is 2 intervals prior to the current one, etc.

— Selecting a specific time is useful when the approximate time at which a specific event occurred is known.

Edit any of the interval or time fields on lines 10, 13, or 16. When Enter is pressed, the values change to the selected range.

To select intervals . . .	You must enter an interval or time on . . .
Occurring on and before a selected interval or time	Line 10. The display will include the selected interval plus the 6 intervals recorded before it.
Bracketing a selected interval or time	Line 13. The display will include the selected interval plus the 3 intervals recorded before it and the 3 intervals recorded after it.
Occurring on and after a selected interval or time	Line 16. The display will include the selected interval plus the 6 intervals recorded after it.

ESF Line Performance Statistics Screen Example



```
main/status/performance/esf                                          9128-II
Device Name: Node A                                          05/26/2000 23:32
                     Network 1 ESF LINE PERFORMANCE STATISTICS
Current Interval Timer                                          ESF Error Events
Near=123    Far = 124                                        Near = 15   Far = 12

                   ---ES--   --UAS--   --SES--   --BES--   --CSS--   -LOFC--
          Time    Near Far  Near Far  Near Far  Near Far  Near Far  Near Far
 Current: 10:37      0   0     0   0     0   0     0   0     0   0     0   0
  Int 01: 10:35      0   0     0   0     0   0     0   0     0   0     0   0
  Int 02: 10:20      0   0     0   0     0   0     0   0     0   0     0   0
  Int 03: 10:05      0   0     0   0     0   0     0   0     0   0     0   0
  Int 04: 09:50      0   0     0   0     0   0     0   0     0   0     0   0
  Int 05: 09:35      0   0     0   0     0   0     0   0     0   0     0   0
  Int 06: 09:20      0   0     0   0     0   0     0   0     0   0     0   0
  Int 07: 09:05      0   0     0   0     0   0     0   0     0   0     0   0

  Worst Interval:   24  24    14  14    14  14    09  09    18  16    44  44
Near Tot(valid 96):  00010     00000     00000     00000       002       003
Far  Tot(valid 96):  00010     00000     00000     00000       002       003

--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Refresh     PgDn   PgUp     ClrFarStats   ClrNearStats
Select: 01, 02, 03, 04, 05, 06, 07, 08, 09 ...
```

For the ESF line performance statistics, the following performance statistics are kept for each 15-minute interval over the past 24-hour period. A Near set and a Far set are kept for each statistic. The Far set is based on information kept by the unit at the other end of the local loop and is only available when ANSI performance report messages are enabled in the unit.

Summary information that appears near the top of the screen includes:

- **Near/Far Current Interval Timer** – Contains the number of seconds that have elapsed in the current 15-minute interval for the near or far information, which can show a value up to 900 seconds.
- **Near/Far ESF Error Events** – Maintains a count of ESF error events, as specified by AT&T TR 54016, which counts CRC and OOF events. A maximum of 65,535 error events can be counted. Once 65535 is reached, it stays at that number until the network issues a reset command.

The following performance statistics are collected for ESF line conditions.

Table 7-21. ESF Line Condition Performance Statistics

Statistic	What It Indicates
Errored Seconds (ES)	Any second with one or more ESF Error events.
Unavailable Seconds (UAS)	Any second in which service is unavailable. Begins incrementing at the onset of 10 consecutive seconds of severely errored seconds (SES), and stops incrementing after 10 consecutive seconds of no SESs.
Severely Errored Seconds (SES)	Any second with 320 or more CRC errors or one or more Out Of Frame (OOF) events.
Bursty Errored Seconds (BES)	Any second with more than one, but less than 320 CRC errors.
Controlled Slip Seconds (CSS)	Any second with one or more controlled slips (a replication or deletion of a DS1 frame by the receiving device). This is collected for network performance statistics only.
Loss of Frame Count (LOFC)	The number of Loss of Frame conditions.
Worst Interval	The largest number of seconds for either ES, UAS, SES, BES, or CSS, or the greatest Loss of Frame Count (LOFC). If more than one interval contains the same worst value, then the oldest interval is displayed.

DBM Call Performance Statistics

When an ISDN DBM is installed, these statistics are available for ISDN calls and call attempts.

You can clear these statistics by selecting the ClrDBMStats function key, or you can clear all performance statistics for the system.

Main Menu→Status→Performance Statistics→Clear All Statistics

Clearing these statistics will not affect performance statistics stored in user history for the system. The statistics are only cleared locally.

Table 7-22. DBM Call Performance Statistics

Statistic	What It Indicates
Total Call Attempts	Number of call attempts made by the DBM.
Total Calls Originated	Number of successful calls made by the DBM.
Total Calls Answered	Number of successful calls answered by the DBM.
Total Calls Rejected (Security)	Number of calls rejected by the DBM due to security.
Total Calls Rejected (Other)	Number of calls rejected by the DBM due to reasons other than security, like incoming voice call requests.
Average Call Duration (mins)	Average amount of time, in minutes, that successful calls take.
Longest Call Duration (mins)	Amount of time spent, in minutes, during the longest successful call.
Total Call Duration (mins)	Sum of all successful calls in minutes.

Ethernet Performance Statistics

The following statistics appear when Ethernet is selected from the Performance Statistics menu.

Main Menu → Status → Performance Statistics → Ethernet

Table 7-23. Ethernet Performance Statistics

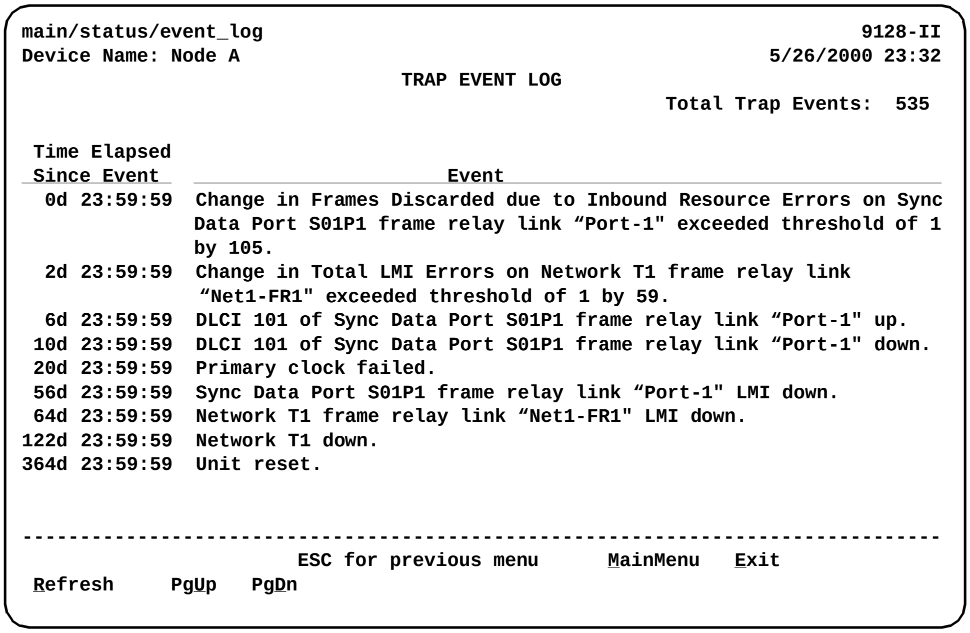
Statistic	What It Indicates
Port Rate (Mbps)	The operating rate as detected on the Ethernet port. One of the following may appear for this statistic: ■ Disconnected – The line is not connected. ■ 10 Mbps or 100 Mbps – The Ethernet port is operating at this rate. ■ Disabled – The Ethernet port has been disabled.
Duplex	The duplex mode detected on the Ethernet port. One of the following may appear for this statistic: ■ Disconnected – The line is not connected. ■ Full – The Ethernet port is operating in full duplex mode (4-wire). ■ Half – The Ethernet port is operating in half duplex mode (2-wire). ■ Disabled – The Ethernet port has been disabled.
Frames Transmitted	The number of successfully transmitted frames on the port.
Frames Received	The number of frames received on the port.
Errored Frames	The number of errors detected on the port. Possible errors include: ■ Internal transmit and receive errors ■ Transmitter and receiver overruns ■ Receive checksum errors ■ Alignment errors ■ Long frames
Excessive Collisions	The number of failed frame transmissions due to excessive collisions.
Carrier Sense Errors	The number of times the carrier sense condition was lost, or was never asserted, during frame transmissions.
Deferred Transmissions	The number of delayed first transmissions due to the line being busy.

Trap Event Log

The Trap Event Log displays all traps stored in the SNMP trap event log. The following log example describes the alarm conditions that will generate an SNMP trap for a physical interface, and for the frame relay LMIs and DLCIs. These alarm conditions also generate Health and Status messages seen on the *Health and Status Messages* on page 7-20.

Main Menu→Status → Trap Event Log

Trap Event Log Screen Example



```
main/status/event_log                                                  9128-II
Device Name: Node A                                           5/26/2000 23:32
                                 TRAP EVENT LOG
                                                      Total Trap Events:  535

 Time Elapsed
 Since Event                          Event
  0d 23:59:59  Change in Frames Discarded due to Inbound Resource Errors on Sync
               Data Port S01P1 frame relay link “Port-1" exceeded threshold of 1
               by 105.
  2d 23:59:59  Change in Total LMI Errors on Network T1 frame relay link
                “Net1-FR1" exceeded threshold of 1 by 59.
  6d 23:59:59  DLCI 101 of Sync Data Port S01P1 frame relay link “Port-1" up.
 10d 23:59:59  DLCI 101 of Sync Data Port S01P1 frame relay link “Port-1" down.
 20d 23:59:59  Primary clock failed.
 56d 23:59:59  Sync Data Port S01P1 frame relay link “Port-1" LMI down.
 64d 23:59:59  Network T1 frame relay link “Net1-FR1" LMI down.
122d 23:59:59  Network T1 down.
364d 23:59:59  Unit reset.



--------------------------------------------------------------------------------
                         ESC for previous menu      MainMenu   Exit
 Refresh     PgUp   PgDn
```

Up to 12 trap events can be displayed on a screen, the most current first. Page down (PgDn) to view less current trap events. When no trap events have been logged, **`No Events in Log.`** appears in the Event column.

ASCII trap strings used to describe trap events are provided in the tables contained in *Standards Compliance for SNMP Traps* in Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*.

Modem Operation

This section includes the following:

- *Activating the Modem PassThru Feature*
- *Canceling Modem PassThru Operationn*
- *Manually Disconnecting the Modem*
- *Verifying Modem Operation*

See *Setting Up the Modem* in Chapter 4, *Configuration Options,* for additional information.

Activating the Modem PassThru Feature

Access to the router's VT100-compatible user interface is provided through the FrameSaver unit's Modem PassThru feature, also known as Router Assist. A dial-up connection to the FrameSaver unit is used to access the router when the unit is set up for this use. See *Setting Up to Use the Modem PassThru Feature* in Chapter 4, *Configuration Options*, to configure the unit for Modem PassThru operation.

Once the unit is set up to use this feature, each time access to the router is needed, the feature is activated from the Control menu.

Main Menu→Control→Enable Modem PassThru to COM

When this feature is active, a logical connection between the unit's modem and COM ports is made, and data received over the modem port is transmitted out the COM port to the router's AUX or console port, and data received from the router on the COM port is transmitted out the modem port. While Modem PassThru is active, normal access to the FrameSaver unit through either its modem or COM port is suspended.

When an escape sequence (minus, minus, minus, with a minimum of 50 ms between each) is detected, the FrameSaver unit switches back to normal user interface operation.

Canceling Modem PassThru Operation

When Modem PassThru is active, but access to the FrameSaver unit's menu-driven user interface is needed, Modem PassThru can be cancelled from the Control menu.

Main Menu→Control→Disable Modem PassThru to COM

Manually Disconnecting the Modem

If Trap Disconnect is disabled, a modem connection remains until it is manually disconnected. Select Disconnect Modem from the Control menu.

Main Menu→Control→Disconnect Modem

Respond yes to the **`Are you sure?`** prompt.

Verifying Modem Operation

▶ Procedure

If Port Use is set to Terminal (dial-in access):

1. Dial the modem's phone number using a remote VT100-compatible asynchronous terminal or PC.
2. Verify that the Main Menu appears.

▶ Procedure

If Port Use is set to Net Link (SNMP, Telnet, FTP, and trap dial-out):

1. Dial the modem's phone number using a PC running PPP or SLIP link protocol.
2. From the PC, run an IP Ping test to the modem interface.

If your results using either method are unsuccessful, make sure both ends of the modem cable are properly seated and secured. Then, verify that the modem was configured correctly (see *Setting Up the Modem* in Chapter 4, *Configuration Options*).

ISDN DBM Operation

The following sections only apply to units with an ISDN DBM:

- *Forcing Backup (Disruptive)*
- *Placing a Test Call (Nondisruptive)*
- *Verifying ISDN Lines*
- *Verifying That Backup Can Take Place*

Forcing Backup (Disruptive)

Use this procedure to force backup when network maintenance is planned, when equipment problems are reported, or when testing the backup path – whenever data needs to be forced from the primary destination interface to the alternate destination, typically from the T1 network to the ISDN.

▶ Procedure

1. Make sure the ISDN Link Profiles are set up correctly, Auto Backup is enabled, and the ISDN interface is enabled (see *Setting Up Dial Backup* in Chapter 4, *Configuration Options*).

2. Have someone at the far end disconnect the network cable to initiate backup.

3. Verify that backup is taking place.

   See *Verifying That Backup Can Take Place* on page 7-74.

   NOTE:

   When an alarm requiring backup is received, backup can be manually controlled by enabling or disabling the Auto Backup option (see Step 2).

4. Have the far-end network cable reconnected to return to standard operation.

Placing a Test Call (Nondisruptive)

Use this procedure to test the ISDN path to each remote site. This procedure will not put the system into backup.

▶ Procedure

1. Make sure the ISDN Link Profiles and DLCIs are set up correctly for the DBMs at each end (see *Modifying ISDN Link Profiles* in Chapter 4, *Configuration Options*.

   Main Menu→Configuration→ISDN→Link Profiles

   Main Menu→Configuration→ISDN→DLCI Records

2. Place a Test Call from one of the devices.

   Main Menu→Test→ISDN Call/PVC Tests

   — Select the link to be tested.

   — Start a Test Call. The Status should be Active.

If the Result is . . .	**Then . . .**
Frame Relay Link Up	The call was successful.
Frame Relay Link Down	The call was not successful. Verify the configuration and Link Status in the ISDN Link Profile.

   — Select Stop to end the Test Call.

Use this procedure to test the ISDN path to each remote site. This procedure will not put the unit into backup.

Verifying ISDN Lines

Use either of the following methods to verify operation of the ISDN lines.

- Check the status of the DBM interface:

  Main Menu→Status→DBM Interface Status

  Line Status should display Active. If an invalid (Inv) status appears (e.g., Inv SPID for an ISDN BRI DBM) in the Line Status field, verify that you entered ISDN physical options correctly.

- Check the status of the unit:

  Main Menu→Status→System and Test Status→
  Health and Status column

  `System Operational` should appear.

  If **`ISDN Network Failed`** appears, check that both ends of the ISDN cable are seated properly for a good physical connection. If that does not clear the message, verify that you entered ISDN physical option information correctly, then contact the network service provider.

See *DBM Interface Status* on page 7-38, and Table 7-8, Health and Status Messages, for additional status information.

Verifying That Backup Can Take Place

As each remote site is installed, verify its backup operation by unplugging the network cable so the system is forced into backup.

- Verify the ISDN lines by checking the DBM Interface Status.

  Main Menu→Status→DBM Interface Status

  Line Status should be Active. If an invalid (Inv) status (e.g., Inv SPID) is displayed, verify that you entered ISDN physical options correctly.

- Check backup setup and that data can be passed between DBMs.
- Reconnect the network cable.

See Table 7-8, Health and Status Messages, *Viewing LEDs and Control Leads* on page 7-4, and *DBM Call Performance Statistics* on page 7-67, for additional information.

FTP File Transfers

The FrameSaver unit supports a standard File Transfer Protocol (FTP) server over Transmission Control Protocol (TCP). A complete binary image of the configuration files can be copied to a host to provide a backup. To use this feature, the unit must be configured to support Telnet and FTP Sessions.

Using this feature, you can transfer configuration files *to/from* a FrameSaver node, program files *to* a FrameSaver node, and User History data *from* a FrameSaver node through a user data port or the network interface using a management PVC, or through the COM port.

Be aware of the following rules when doing a file transfer:

- You must have Access Level 1 permission to use the **put** and **get** commands, and to access the LMI packet capture data. However, you can retrieve the data file for the user history reports regardless of access level.
- You cannot **put** a configuration file to the factory.cfg or current.cfg files under the system directory. Configuration files should be put to a customer file (cust1.cfg or cust2.cfg), then loaded into the downloaded unit's Current Configuration via the menu-driven user interface.
- You can only **put** a NAM program file (nam.ocd) into a FrameSaver unit. You cannot **get** a program file from the FrameSaver unit to a host.
- Before putting a download file, you must use the **bin** binary command to place the data connection in binary transfer mode.
- When transferring SLV user history information to the NMS, you can only **get** a uhbcfull.dat file. It is recommended that you use the NMS application to get this information (see *Transferring Collected Data* on page 7-80).
- A data file (uhbcfull.dat or lmitrace.syc) cannot be **put** into a FrameSaver node.
- LMI packet capture data (lmitrace.syc) is not readable when the LMI Packet Capture Utility is active.

FrameSaver SLV units provide an additional feature that allows new software to be downloaded in the background, using the selected bandwidth and without interfering with normal operation. Downloads can be performed quickly, using the full line speed, or at a slower rate over an extended period of time.

You initiate an FTP session to a FrameSaver node in the same way as you would initiate an FTP to any other IP-addressable device.

NOTE:

Loading a configuration with many DLCIs from a unit's Customer Configuration 1 or 2 option area into its Current Configuration area may take time. Allow a minute or more for the downloaded file to be put into the unit's currently active configuration.

▶ Procedure

To initiate an FTP session:

1. Start the FTP client program on your host. For example, on a UNIX host, type **ftp**, followed by the FrameSaver unit's IP address.

2. If a login and password are required (see *Creating a Login* in Chapter 6, *Security and Logins*), you are prompted to enter them. If not, press Enter.

   The FTP prompt appears.

   The starting directory is the root directory (/). Use standard FTP commands during the FTP session, as well as the following remote FTP commands.

Command	Definition
cd *directory*	Change the current directory on the FrameSaver node to the specified *directory.*
dir [*directory*]	Print a listing of the directory contents in the specified *directory.* If no directory is specified, the current one is used.
get *file1* [*file2*]	Copy a file from the remote directory of the FrameSaver node to the local directory on the host (for configuration files only).
remotehelp [*command*]	Print the meaning of the command. If no argument is given, a list of all known commands is printed.
ls [*directory*]	Print an abbreviated list of the specified directory's contents. If no directory is specified, the current one is used.
put *file1* [*file2*]	Copy *file1* from a local directory on the host to *file 2* in the current directory of the FrameSaver node. If *file2* is not specified, the file will be named *file1* on the FrameSaver node.
recv *file1* [*file 2*]	Same as a **get**.
send *file1* [*file 2*]	Same as a **put**.
pwd	Print the name of the current directory of the FrameSaver unit node.
bin	Places the FTP session in binary-transfer mode.

Upgrading System Software

If you need to upgrade the FrameSaver unit's program code, you must transfer the upgrade of the **nam.ocd** file in the system memory directory using the **put** command.

NOTE:

Upgrades can be performed through the network using a Management PVC, or through the COM port if Port Use is set to Net Link (see Table 4-23, Ethernet Management Options, in Chapter 4, *Configuration Options*).

▶ Procedure

To download software:

1. Initiate an FTP session to the device that you are upgrading.
2. Type **bin** to enter binary transfer mode.
3. Type **hash** to enter hash mode if you want to monitor the progress of the upgrade, provided this function is supported by your equipment.
4. Type **cd system** to change to the system directory.
5. Perform a **put** of R*xxxxxx*.ocd (*xxxxxx* being the software release number) to the nam.ocd file to start the upgrade.

If the message displayed is . . .	Then . . .
nam.ocd: File Transfer Complete	The download was successful. The file is loaded into system memory.
nam.ocd: File Transfer Failed – Invalid file	The file is not valid for this FrameSaver unit. A different R*xxxxxx*.ocd file will need to be downloaded. Repeat the step or end the FTP session.

NOTE:

During the download, a series of hash marks (#) appear. When the hash marks stop appearing, there is a pause of about 30 seconds before the `nam.ocd: File Transfer Complete` message appears. Please be patient. Do not exit from FTP at this time.

See *Changing Software* on page 7-79 to activate the newly downloaded software.

Upgrading ISDN BRI DBM Software

A separate download to update PRI DBM functionality is not necessary; a PRI upgrade is incorporated in the unit's program code. However, if the FrameSaver unit has a BRI DBM, the program code must be upgraded separately.

To upgrade a FrameSaver unit's BRI DBM program code, you must transfer the **dbmprog.ocd** file in the Dial Backup Module directory using the **put** command.

▶ Procedure

To perform a BRI DBM upgrade:

1. Initiate an FTP session to the device that you are upgrading.
2. Type **bin** to enter binary transfer mode.
3. Type **cd dbm** to change to the Dial Backup Module directory.

   NOTE:

   If the FrameSaver unit is not equipped with a DBM or the DBM does not contain any downloadable software, the message **`dbm: no such file or directory`** appears.

4. Perform a **put** of R*xxxxxx*.ocd (*xxxxxx* being the software release number) to the dbmprog.ocd file to start the upgrade.

If the message displayed is . . .	Then . . .
DBM Download Required	Errors were detected during the DBM download. The dbmprog.ocd file will need to be downloaded again.
dbmprog.ocd: File Transfer Complete	The download was successful.
dbmprog.ocd: File Transfer Failed	The download was not successful. Possible cause: A bad or invalid file, or the wrong checksum. A different dbmprog.ocd file will need to be downloaded for the DBM to become operational. Repeat the step or end the FTP session.

5. Close the FTP session.
6. Verify that the new software release was successfully installed as the DBM Software Revision.

   Main Menu→Status→Identity

Determining Whether a Download Is Completed

To see whether a download has completed, check the Identity screen.

Main Menu→Status→Identity

Check Alternate Software Rev. under the NAM Identity column.

- If a software revision number appears, the file transfer is complete.
- If **`In Progress`** appears, the file is still being transferred.
- If **`Invalid`** appears, no download has occurred or the download was not successful.

Changing Software

Once a software upgrade is downloaded, it needs to be activated. When activated, the unit resets, then executes the downloaded software. With this feature, you control when the upgrade software is implemented.

▶ Procedure

To switch to the new software:

1. Go to the Control menu, and select Select Software Release.

   Main Menu→Control→Select Software Release

   The currently loaded software version and the new release that was just transferred are shown.

   If the download failed, **`Invalid`** appears in the Alternate Release field instead of the new release number. Repeat the procedure *Upgrading System Software* if this occurs.

2. Select S<u>w</u>itch&Reset.

3. Enter <u>Y</u>es to the **`Are you sure?`** prompt. The unit resets and begins installing the newly transferred software.

4. Verify that the new software release was successfully installed as the Current Software Revision.

   Main Menu→Status→Identity

   NOTE:

   If someone opens a Telnet session and accesses the unit's Identity screen while the unit is downloading software, the **`In Progress...`** message appears in the Alternate Software Revision field.

   See *Displaying System Information* on page 7-3 to see what is included on the unit's Identity screen.

Transferring Collected Data

SLV user history statistics and LMI packet capture data can be uploaded to an NMS or a Network Associates Sniffer using FTP, which is faster than other methods. The rate at which the data file is transferred is the rate set by the FTP Max Transfer Rate (Kbps) option (see Table 4-20, Telnet and FTP Session Options, in Chapter 4, *Configuration Options*).

NOTE:

Use your NMS application to FTP and view transferred statistics and packet data; the data files are not in user-readable format. LMI packet capture data can also be viewed via the LMI Trace Log (see *Viewing Captured Packets from the Menu-Driven User Interface* in Chapter 8, *Troubleshooting*, for additional information).

▶ Procedure

To retrieve data:

1. Initiate an FTP session to the device from which SLV statistics or packet data will be retrieved.
2. Type **bin** to enter binary transfer mode.
3. Type **hash** to enter hash mode if you want to monitor the progress of the upgrade, provided this function is supported by your equipment.
4. Type **cd data** to change to the data directory.

If retrieving . . .	Then . . .
SLV statistics	Perform a **get** of the **uhbcfull.dat** file. ■ **`File Transfer Complete`** – Transfer was successful. ■ **`File Transfer Failed`** – Transfer was not successful. Try again or end the session.
LMI packet capture data	1. Stop the LMI Packet Capture Utility. *Main Menu→Control→LMI Packet Capture Utility* LMI packet capture data is not available (readable) when the LMI Packet Capture Utility is Active. 2. Perform a **get** of the **lmitrace.syc** file. One of the following will display for the file: – **`File Transfer Complete`** – **`File Transfer Failed`** – **`Permission Denied`** – The LMI Packet Capture Utility was not readable. Stop the LMI Packet Capture Utility and try again.

5. Close the FTP session.

SLV statistics and/or LMI Packet Capture data are now available for reporting.

Turning Off the System Alarm Relay

For carrier-mounted FrameSaver units, an alarm system relay is provided by the 9000 Series Access Carrier. This relay activates a light or buzzer when an alarm condition is detected in one of the FrameSaver units.

Once the alarm relay is connected, enabling the System Alarm Relay option activates this feature (see Table 4-5, General System Options, in Chapter 4, *Configuration Options*).

Once activated, the relay is turned off in one of the following ways:

- The alarm condition that activated the relay no longer exists. The relay stays on until all alarm conditions have been corrected.
- The System Alarm Relay option can be disabled.

  Main Menu → Configuration → System → General

- System Alarm Relay Cut-Off can be selected.

  Main Menu → Control → System Alarm Relay Cut-Off

See *Alarm Relay Connector* in the *9000 Series Access Carrier Installation Instructions* for information about connecting the alarm relay.

Troubleshooting

8

This chapter includes the following:

- *Physical Tests* on page 8-26
  - *Line Loopback*
  - *Payload Loopback*
  - *Repeater Loopback*
  - *DTE Loopback*
  - *Send Line Loopback*
  - *Data Channel Loopbacks on a Frame Relay Link*
  - *Send Remote Line Loopback*
  - *Send and Monitor Pattern Tests*
- *IP Ping Test* on page 8-35
- *Lamp Test* on page 8-40

Problem Indicators

The unit provides a number of indicators to alert you to possible problems:

Indicators . . .	See . . .
LEDs	*Viewing LEDs and Control Leads* and *LED Descriptions* in Chapter 7, *Operation and Maintenance*, as well as the user interface screen. *Main Menu→ Status→ Display LEDs and Control LEDs*
Health and Status	Table 7-8, Health and Status Messages, in Chapter 7, *Operation and Maintenance*. *Main Menu→ Status→ System and Test Status* Messages also appear at the bottom of any menu-driven user interface screen.
Performance statistics	*Performance Statistics* in Chapter 7, *Operation and Maintenance*, to help you determine how long a problem has existed.
Alarm conditions that will generate an SNMP trap	*Alarms* on page 8-7.
SNMP traps	Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults.* Traps supported include warm-start, authentication-failure, enterprise-specific (those specific to the unit), link-up, and link-down.

Resetting the Unit and Restoring Communication

You can reset the unit in one of four ways:

- Reset it from the Control menu.
- Cycle the power.
- Reset the configuration options for the COM port, or reload the factory default settings.
- Set the appropriate MIB object from NMS (see your NMS documentation).

The unit performs a self-test when it is reset.

Resetting the Unit from the Control Menu

Use this procedure to initiate a reset and power-on self-test of the unit.

▶ **Procedure**

To reset the unit from the Control menu:

1. From the Main Menu screen, select Control.
2. Select Reset Device and press Enter. The **`Are You Sure?`** prompt appears.
3. Type **`y`** (Yes) and press Enter. The unit reinitializes itself, performing a self-test.

Resetting the Unit By Cycling the Power

Disconnecting, then reconnecting the power cord resets the unit.

Restoring Communication with an Improperly Configured Unit

Configuring the unit improperly could render the menu-driven user interface inaccessible. If this occurs, connectivity to the unit can be restored via a directly connected asynchronous terminal.

▶ Procedure

To reset COM port settings:

1. Configure the asynchronous terminal to operate at 19.2 Kbps, using character length of 8 bits, with one stop-bit, and no parity. In addition, set Flow Control to None.
2. Reset the unit, then hold the Enter key down until the System Paused screen appears. (See *Resetting the Unit and Restoring Communication* on page 8-3 for other methods of resetting the unit.)
3. Tab to the desired prompt, and type **y** (Yes) at one of the prompts.

If selecting . . .	The following occurs . . .
Reset COM Port usage	■ Port Use is set to Terminal so the asynchronous terminal can be used. ■ Data Rate (Kbps), Character Length, Stop Bits, and Parity are reset to the factory defaults. ■ Unit resets itself.
Reload Factory Defaults	■ All configuration and control settings are reset to the Default Factory Configuration, overwriting the current configuration. ■ Unit resets itself. **CAUTION**: This causes the current configuration to be destroyed and a self-test to be performed.

If no selection is made within 30 seconds, or if No (**n**) is entered, the unit resets itself and no configuration changes are made.

Once the unit resets itself, connectivity is restored and the Main Menu screen appears.

Troubleshooting Management Link Feature

A dedicated troubleshooting management link is available to help service providers isolate device problems within their networks. This feature allows Telnet or FTP access to the unit on this link and troubleshooting over this link is essentially transparent to customer operations. No alarms or SNMP traps are generated to create nuisance alarms for the customer.

See *Configuring Node IP Information* in Chapter 4, *Configuration Options*, for additional information about this feature.

LMI Packet Capture Utility Feature

A packet capture utility has been provided to aid with problem isolation when LMI errors are detected. Using this utility, any enabled frame relay link on the user data port or network interface can be selected. The utility captures any LMI packets sent or received and writes them to a data file called lmitrace.syc in the system's data directory so the data can be uploaded and transferred to a Network Associates Sniffer for analysis.

The LMI Trace Log also provides access to captured packet information. See *Viewing Captured Packets from the Menu-Driven User Interface* on page 8-6 for additional information on this feature.

▶ Procedure

To use this utility:

1. Select the LMI Packet Capture Utility. Select an enabled frame relay link.

   Main Menu→Control→LMI Packet Capture Utility

2. Select an enabled frame relay link, or Capture Interface, either Net1-FR1 Port-1, Port-2, or an ISDN Link Name if a DBM is present.

3. Start packet capture.

   While capturing data, the status is Active. Packets in Buffer indicates the number of packets that have been captured. Up to 8000 packets can be held. When the buffer is full, the oldest packets will be overwritten.

4. To stop the utility, press Enter. The field toggles back to Start.

5. Upload the data file holding the collected packets to a diskette so the information can be transferred to a Network Associates Sniffer for debugging/decoding.

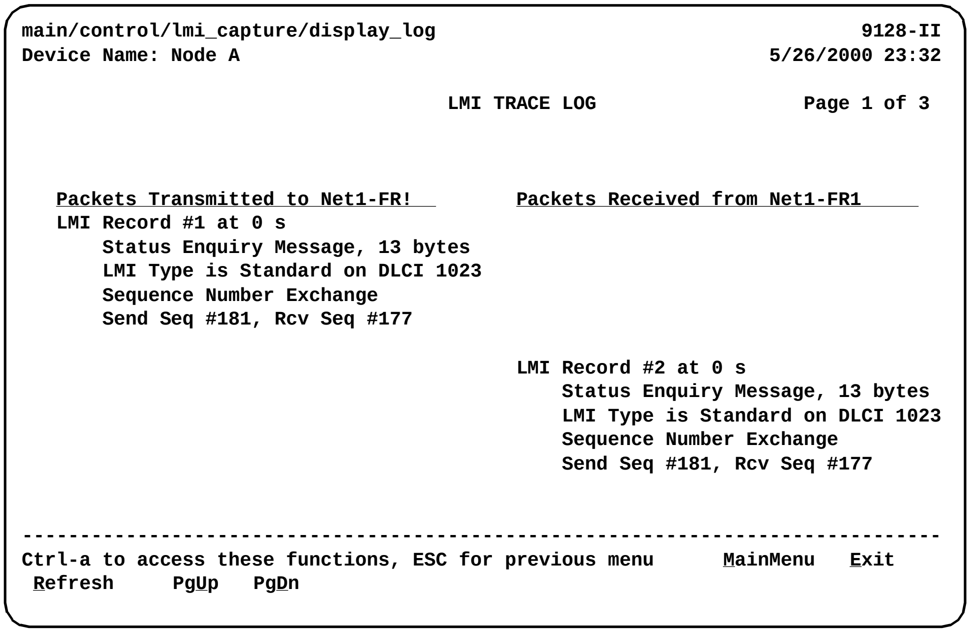
See *Transferring Collected Data* in Chapter 7, *Operation and Maintenance*, for additional information about this feature.

Viewing Captured Packets from the Menu-Driven User Interface

The twelve most recent LMI events are stored in the trace log. Once the capture buffer or trace log is full, the oldest packets are overwritten. To view the most recently captured packets using the menu-driven user interface:

LMI Packet Capture Utility→Display LMI Trace Log

LMI Trace Log Example



```
main/control/lmi_capture/display_log                                     9128-II
Device Name: Node A                                              5/26/2000 23:32

                                     LMI TRACE LOG                  Page 1 of 3



   Packets Transmitted to Net1-FR!         Packets Received from Net1-FR1
   LMI Record #1 at 0 s
       Status Enquiry Message, 13 bytes
       LMI Type is Standard on DLCI 1023
       Sequence Number Exchange
       Send Seq #181, Rcv Seq #177

                                           LMI Record #2 at 0 s
                                               Status Enquiry Message, 13 bytes
                                               LMI Type is Standard on DLCI 1023
                                               Sequence Number Exchange
                                               Send Seq #181, Rcv Seq #177


--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 Refresh     PgUp   PgDn
```

Select Refresh to update the screen with the twelve most recently collected LMI messages.

The following information is provided:

- The internal LMI record number assigned to the packet (1–8000), and the amount of time the utility was running when the packet was captured.

  The maximum amount of time displayed is 4,294,967 seconds (s), which is reset to 1 second when this amount of time is exceeded.

- The type of message, either Status or Status Enquiry, from the captured packet, and the number of bytes in the packet.
- The LMI Type identified in the Protocol Discriminator portion of the captured packet, and the DLCI number for the packet.
- The type of information contained in the captured packet, either Sequence Number Exchange or Full Status Report.
- The send and receive (rcv) sequence numbers from the captured packet (0–255).
- On the Packets Received side of the screen, PVC status for up to ten DLCIs can be shown. It shows the DLCI number, its active bit status, and if Standard LMI is running, the DLCI's CIR value.

Alarms

The following table describes the alarm conditions that will generate an SNMP trap for a physical interface, and the frame relay LMIs and DLCIs. These alarm conditions also generate Health and Status messages seen on the System and Test Status screen.

Main Menu→Status →System and Test Status

Table 8-1. Alarm Conditions (1 of 7)

Alarm Condition	What It Indicates	What To Do
AIS at DSX-1	For the DSX-1 interface, the attached DTE is transmitting an AIS.	For the DSX-1 interface, check the DTE attached to the interface.
AIS at Network 1	An Alarm Indication Signal (AIS) is being received by the interface. AIS is an unframed, all ones signal.	For the network interface, report the problem to your T1 service provider.
CTS down to Port-1 Device	The CTS control lead on the device's interface is off.	Check DTR and RTS from Port-1. ■ Verify that the port is enabled. ■ Check DTR from the user data port.
DBM BRI Card Failed	The ISDN BRI DBM failed to pass the self-test.	Reset the FrameSaver unit (*Main Menu→ Control→ Reset Device).* If the DBM fails again, contact your service representative.
DLCI *nnnn* Down, *frame relay link*[1,2]	The DLCI for the specified frame relay link is down.	Verify that the network LMI is up. If it is, contact your network provider, or your ISDN service provider if an ISDN Link Name is the link.
DTR Down from Port-1 Device	The DTR control lead on the device connected to Port-*n* is disasserted. The DTR control lead on the device connected to the specified port is off. This message applies to data ports that act as DCEs.	Examine the attached DTE and cable connected to the system's port. ■ Check that the port cable is securely attached at both ends. ■ Check the status of the attached equipment.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with a user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Access Management Link DLCI.

Table 8-1. Alarm Conditions (2 of 7)

Alarm Condition	What It Indicates	What To Do
EER at Network 1	The error rate of the received network signal exceeds the currently configured threshold. This condition only occurs if the network interface is configured for ESF framing. This condition clears when the error rate falls below the threshold value, which may take up to 15 minutes.	■ Verify that the network cable is securely attached at the network interface. ■ Contact your network provider.
Ethernet Link Down	The communication link for the Ethernet port is down and the Interface Status for the port is enabled.	Check the LAN connected to the Ethernet port.
Internal Modem Failed	The unit's internal modem failed to pass the self-test.	Reset the FrameSaver unit (*Main Menu→ Control→ Reset Device)*. If the modem fails again, contact your service representative.
ISDN Link Profile Disabled *ISDN Link Name*	An ISDN backup call could not be made because the ISDN link profile specified Link Name is disabled (*Main Menu→ Configuration→ ISDN→ Link Profiles)*.	Enable the ISDN link profile if you want to make a call.
ISDN Link Profile Invalid, *ISDN Link Name*	An ISDN backup call could not be made because the ISDN link profile specified (*ISDN Link Name*) is invalid.	Check that the phone number is correct.
ISDN Network Failed (Active/Idle)	An ISDN network failure was detected when a backup call was in progress or the DBM was in Idle mode.	Contact your network provider if the problem persists.
LatExceed-*IP_Address,* COS*x*,DLCI*nnnn*[1]	An IP SLV Latency Threshold has been exceeded for the specified Class Of Service of the path.	Contact your service provider.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with a user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Access Management Link DLCI.

Table 8-1. Alarm Conditions (3 of 7)

Alarm Condition	What It Indicates	What To Do
Link Profile Disabled, *ISDN Link Name*	An ISDN backup call could not be made because the specified link profile was disabled.	Change the ISDN Link Profile's Link Status to Auto (*Main Menu→ Configuration→ ISDN→ Link Profiles)*.
LMI Down, *frame relay link*[2]	The Local Management Interface is down for the specified frame relay link.	For the network interface: ■ If LMI was never up, verify that the LMI Protocol setting reflects the LMI type being used. ■ If LMI was never up: – Verify that the proper time slots have been configured. – Verify that the LMI Protocol setting reflects the LMI type being used. ■ Verify that Frame Relay Performance Statistics show LMI frames being transmitted. If all of the above have been verified and the physical link is not in Alarm, contact your network provider.
		For user data port: ■ Check that the DTE cable is securely attached at both ends. ■ Verify that Transmit Clock Source and Invert Transmit Clock options are properly configured. ■ Verify that Frame Relay Performance Statistics show LMI frames being received. If no frames are being received: – Check the attached device. – Verify that the LMI Protocol setting reflects the LMI type being used.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with a user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Access Management Link DLCI.

Table 8-1. Alarm Conditions (4 of 7)

Alarm Condition	What It Indicates	What To Do
LOS at DSX-1	A Loss of Signal (LOS) condition is detected on the DSX-1 interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%.	
	■ DSX-1 cable problem.	■ Check that the DSX-1 cable is securely attached at both ends.
	■ No signal being transmitted from the DTE.	■ Check the DTE status.
LOS at Network 1	A Loss of Signal (LOS) condition is detected on the network interface. Clears when the ratio of ones to zeros received is greater than or equal to 12.5%.	
	■ Network cable problem.	■ Check that the network cable is securely attached at both ends.
	■ No signal is being transmitted at the far-end FrameSaver unit.	■ Check far-end FrameSaver unit status.
	■ T1 facility problem.	■ Contact your network provider.
Network Com Link Down	The communication link for the COM port is down and the COM port is configured for Net Link.	Check the router connected to the COM port.
OOF at DSX-1	An Out of Frame (OOF) condition is detected on the DSX-1 interface.	
	■ Incompatible framing format between the DTE and the FrameSaver unit.	■ Check that the framing format for the DSX-1 (DTE) interface is correct.
	■ DSX-1 cabling problem.	■ Check that the DSX-1 cable is securely attached at both ends.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with a user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Access Management Link DLCI.

Table 8-1. Alarm Conditions (5 of 7)

Alarm Condition	What It Indicates	What To Do
OOF at Network 1	An Out of Frame (OOF) condition is detected on the network interface. ■ Incompatible framing format between the network and the FrameSaver unit. ■ Network cabling problem. ■ T1 facility problem.	■ Check that the framing format for the network interface is correct. ■ Check that the network cable is securely attached at both ends. ■ Contact your network provider.
Path*IP_ Address* Down, DLCI*nnnn*[1]	A path on the network interface is unavailable.	Determine why the path went down.
Power Supply/Fan Alarm	The power supply output voltage has dropped below the specified tolerance level required for the system. Or one or both fan trays are not operating properly.	Check the LEDs on the power supply and fan trays to determine which may have failed, then replace the failed component.
Primary Clock Failed	A failure of the configured primary clock source for the unit was detected and the secondary clock is providing the timing for the unit. This condition clears when the configured primary clock is restored.	■ Check that the network cable is securely attached at both ends. ■ Contact your network provider.
Primary & Secondary Clocks Failed	A failure of both clock sources configured for the unit was detected. This condition only applies to T1 network and DSX-1 interfaces. It clears when the configured primary clock is restored.	

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with a user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Access Management Link DLCI.

Table 8-1. Alarm Conditions (6 of 7)

Alarm Condition	What It Indicates	What To Do
Secondary Clock Failed	A failure of the configured secondary clock source for the unit was detected and the internal clock is providing the timing for the unit. The clock source will not automatically switch from internal until the primary clock source returns.	
Self-Test Failure	The unit did not pass its basic verification tests when it was powered on or reset.	■ Reset the unit. ■ Contact your service representative.
SLV Latency Exceeded, DLCI *nnnn*, *frame relay link*[1, 2, 3]	The measured latency of SLV communication responses from the remote unit on this DLCI is excessive, so the DLCI has been declared unsuitable for normal multiplexed PVC operation (DLCI Type is set to Multiplexed).	Wait until the DLCI is declared operational again. If the unit has ISDN backup capability, this condition will initiate backup.
SLV Timeout, DLCI *nnnn*, *frame relay link*[1, 2, 3]	An excessive number of SLV communication responses from the remote system have been missed on the specified multiplexed DLCI and link. If the frame relay link is Net1-FR1, the timeout is on the network FrameRly1 timeslot assignment. When a hardware bypass-capable device has been detected at the other end of the PVC and this condition occurs, only user data for EDLCI 0 will be transmitted as long as the condition exists.	■ Verify that the network LMI is up. If it is, contact your network service provider. ■ If a DBM is present and Auto Backup is enabled, backup is initiated automatically.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with a user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Access Management Link DLCI.

Table 8-1. Alarm Conditions (7 of 7)

Alarm Condition	What It Indicates	What To Do
Suboptimal Link Rate, *frame relay link*[2]	The specified frame relay multilink has failed to achieve the configured Maximum Link Rate for the link. This message appears for multilink aggregate frame relay links if LMI is down on any of its constituent links.	No action required.
Two Level-1 Users Accessing Device	Another user with Level-1 security access is currently accessing the unit. Be aware that actions of the other user may override your test commands and configuration changes.	Wait until no other Level-1 users are accessing the unit if testing or configuration will be performed.
Yellow at DSX-1	A yellow alarm signal is received on the DSX-1 interface. DTE has detected a LOS or OOF condition.	■ Check that the DSX-1 cable is securely attached at both ends. ■ Check the status of the attached equipment.
Yellow at Network 1	A yellow alarm signal is received on the network interface. ■ Network cable problem. ■ T1 facility problem.	■ Check that your network cable is securely attached at both ends. ■ Contact your network provider.

[1] *nnnn* indicates a DLCI number of 16 through 1007.

[2] *frame relay link* is one of the following:
– Net1-FR1. The frame relay link specified for the network interface, Network 1.
– Port-*n*. The frame relay link associated with a user data port.
– *ISDN Link Name* on a non-network ISDN DBM interface.

[3] Does not apply to a TS Access Management Link DLCI.

Viewing the Trap Event Log

The Trap Event Log displays all traps stored in the SNMP trap event log. ASCII trap strings used to describe trap events are provided in the tables contained in *Standards Compliance for SNMP Traps* (see Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*).

See *Trap Event Log* in Chapter 7, *Operation and Maintenance*, for a screen example and additional information.

Troubleshooting Tables

The unit is designed to provide many years of trouble-free service. However, if a problem occurs, refer to the appropriate table in the following sections for possible solutions.

Device Problems

Table 8-2. Device Problems (1 of 2)

Symptom	Possible Cause	Solutions
No power, or the LEDs are not lit.	The power cord is not securely plugged into the wall receptacle to rear panel connection.	Check that the power cord is securely attached at both ends.
	The wall receptacle has no power.	■ Check the wall receptacle power by plugging in some equipment that is known to be working. ■ Check the circuit breaker. ■ Verify that your site is not on an energy management program.
Power-On Self-Test fails. Only Alarm LED is on after power-on.	The unit has detected an internal hardware failure.	■ Reset the unit and try again. ■ Contact your service representative. ■ Return the unit to the factory (refer to *Warranty, Sales, Service, and Training Information* on page A of this document).

Table 8-2. Device Problems (2 of 2)

Symptom	Possible Cause	Solutions
Cannot access the unit or the menu-driven user interface.	Login or password is incorrect, COM port is misconfigured, or the unit is otherwise configured so it prevents access.	■ Reset the unit (see *Restoring Communication with an Improperly Configured Unit* on page 8-4). ■ Contact your service representative.
Failure *xxxxxxxx* appears at the top of the System and Test Status screen, at Self-Test Results.	The unit detects an internal software failure.	■ Record the 8-digit code from the System and Test Status screen. ■ Reset the unit and try again. ■ Contact your service representative and provide the 8-digit failure code.
An LED appears dysfunctional.	LED is burned out.	Run the Lamp Test. If the LED in question does not flash with the other LEDs, then contact your service representative.
Not receiving data.	Network cable loose or broken.	■ Reconnect or repair the cable. ■ Call the network service provider.
Receiving data errors on a multiplexed DLCI, but frame relay is okay.	Frame Relay Discovery is being used for automatic DLCI and PVC configuration. The equipment at the other end is not frame relay RFC 1490-compliant.	Change the DLCI Type for each network DLCI from Multiplexed to Standard, turning off multiplexing.

Frame Relay PVC Problems

Table 8-3. Frame Relay PVC Problems

Symptom	Possible Cause	Solutions
No receipt or transmission of data	Cross Connection of the DLCIs are configured incorrectly.	Verify the PVC connections and DLCIs by checking the network-discovered DLCIs on the LMI Reported DLCIs screen.
	DLCI is inactive on the frame relay network.	■ Verify that the DLCI(s) is active on the LMI Reported DLCIs screen. If the DLCI(s) is not active, contact the service provider. ■ Verify the LMI Reported DLCI field on the Interface Status screen.
	DTE is configured incorrectly.	Check the DTE's configuration.
	LMI is not configured properly for the DTE or network.	Configure LMI characteristics to match those of the DTE or network.
	LMI link is inactive.	Verify that the LMI link is active on the network; the Status Msg Received counter on the Network Frame Relay Performance Statistics screen increments.
Losing Data	Frame relay network is experiencing problems.	Run PVC Loopback and Pattern tests to isolate the problem, then contact the service provider.
Out of Sync	If Monitor Pattern was selected, it means the test pattern generator and receiver have not yet synchronized. CIR settings for the units at each end are mismatched. If the message persists, it means that 5 packets out of 25 are missing or are out of sequence.	■ Verify that the unit at the other end is configured to Send Pattern. Correct unit configurations. ■ Correct the CIR setting so both units are configured the same. ■ Check the line's error rate – the physical line quality. Contact the service provider.

ISDN DBM Problems

Table 8-4. ISDN DBM Problems

Symptom	Possible Cause	Solutions
Cannot connect to the remote unit	Misconfiguration	■ Verify that the link profiles are correct in both units, both the area codes and phone or ID numbers (see *Setting Up ISDN Link Profiles* in Chapter 4, *Configuration Options*). ■ For a BRI DBM, verify that the SPIDs and local area codes and phone numbers are correct (see *Configuring the ISDN DBM Interface* in Chapter 4, *Configuration Options*). ■ Verify that the unit at one end is configured to originate and the unit at the other end is configured to answer a call. ■ Verify that the ISDN interface is enabled. ■ Verify that Auto Backup is enabled and no time restrictions apply.
DBM LMI comes up, but no data is transferred	Misconfiguration	Check that the DLCI numbers are correct and are the same at both ends.

See Table 7-14, Most Recent and Previous Cause Value Messages, in Chapter 7, *Operation and Maintenance*, for additional information about ISDN problems. Last Cause Value messages appear on the DBM Interface Status screen.

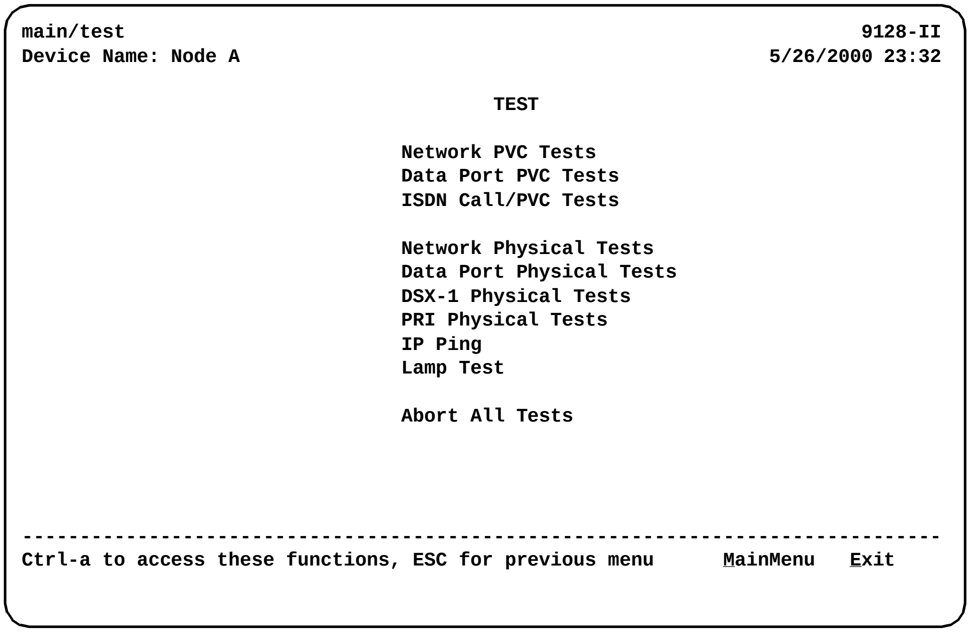
Main Menu→Status →DBM Interface Status

See *Configuring the ISDN DBM Interface* and *Setting Up ISDN Link Profiles* in Chapter 4, *Configuration Options*, for more information about ISDN DBM configuration.

Tests Available

The following tests are available to a FrameSaver SLV 9126, 9128, or 9128-II.

Test Menu Example



```
main/test                                                              9128-II
Device Name: Node A                                            5/26/2000 23:32

                                        TEST

                                Network PVC Tests
                                Data Port PVC Tests
                                ISDN Call/PVC Tests

                                Network Physical Tests
                                Data Port Physical Tests
                                DSX-1 Physical Tests
                                PRI Physical Tests
                                IP Ping
                                Lamp Test

                                Abort All Tests




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

If the unit does not have the ISDN DBM feature, **`ISDN Call`** does not appear with the ISDN PVC Tests. **`PRI Physical Tests`** only appears when an ISDN PRI DBM is installed.

PVC Tests menu selections are suppressed when no PVCs have been configured on the interface. Check that both ends of the cables are properly seated and secured.

Tests can be commanded from the OpenLane 5.*x* management system using its Diagnostic Troubleshooting graphical interface, as well as from the menu-driven user interface.

Test Timeout Feature

A Test Timeout feature is available to automatically terminate a test (as opposed to manually terminating a test) after it has been running a specified period of time.

It is recommended that this feature be used when the FrameSaver unit is remotely managed through an inband data stream (PVC). If a test is accidently commanded to execute on the interface providing management access, control is regained when the specified time period expires, automatically terminating the test.

To use this feature, enable the Test Timeout configuration option, and set a duration for the test to run in the Test Duration (min) configuration option (see *Configuring General System Options* in Chapter 4, *Configuration Options*).

NOTE:

These configuration options do not pertain to tests commanded by the DTE, like a DTE-initiated External Loopback.

DBM Tests

The Test menu allows you to run PVC loopbacks and test patterns on the unit and its DBM interface. It is available to users with a security access level of 1 or 2. Currently, there are no physical tests for a BRI DBM interface.

DBM tests are started and monitored the same as the network tests. See *System and Test Status Messages* in Chapter 7, *Operation and Maintenance*, for ISDN backup-related test messages appearing on the System and Test Status screen. See *PVC Tests* on page 8-22 on for additional information.

Starting and Stopping a Test

Use this procedure to start, monitor, or abort specific tests. To abort all active tests on all interfaces, see *Aborting All Tests* on page 8-21.

When the status of a test is . . .	The only command available is . . .
Inactive	Start
Active	Stop

Start or stop an individual test using the same procedure.

▶ Procedure

To start and stop a loopback or a send-pattern test:

1. Follow this menu selection sequence:

   Main Menu→Test

2. Select an interface and test (e.g., Network, Data Port, or ISDN PVC Tests) and press Enter.

   The selected test screen appears. **`Start`** appears in the Command column. **`Inactive`** appears in the Status column.

3. Select the Port number and press Enter.

4. Select the DLCI number and press Enter if a PVC test has been selected.

   The cursor is positioned at Start in the Command column of the first available test and is highlighted.

5. To start the test, highlight **`Start`** under Command for the test you want to run and press Enter. **`Stop`** now appears and is highlighted, and the status of the test changes to **`Active`**.

   The length of time that the test has been running is shown in the Result column.

6. To stop the test, press Enter to send the Stop command. **`Start`** reappears and the status of the test changes back to **`Inactive`**.

Aborting All Tests

Use the Abort All Tests selection from the Test menu to abort all tests running on all interfaces, with exception to DTE-initiated loopbacks. To abort individual tests that are active, see *Starting and Stopping a Test* on page 8-20.

▶ Procedure

To abort all tests on all interfaces:

1. Follow this menu selection sequence:

   Main Menu→Test

2. Select Abort All Tests and press Enter.

   `Command Complete` appears when all tests on all interfaces have been stopped.

   NOTE:

   Abort All Tests does not interrupt DTE-initiated loopbacks.

PVC Tests

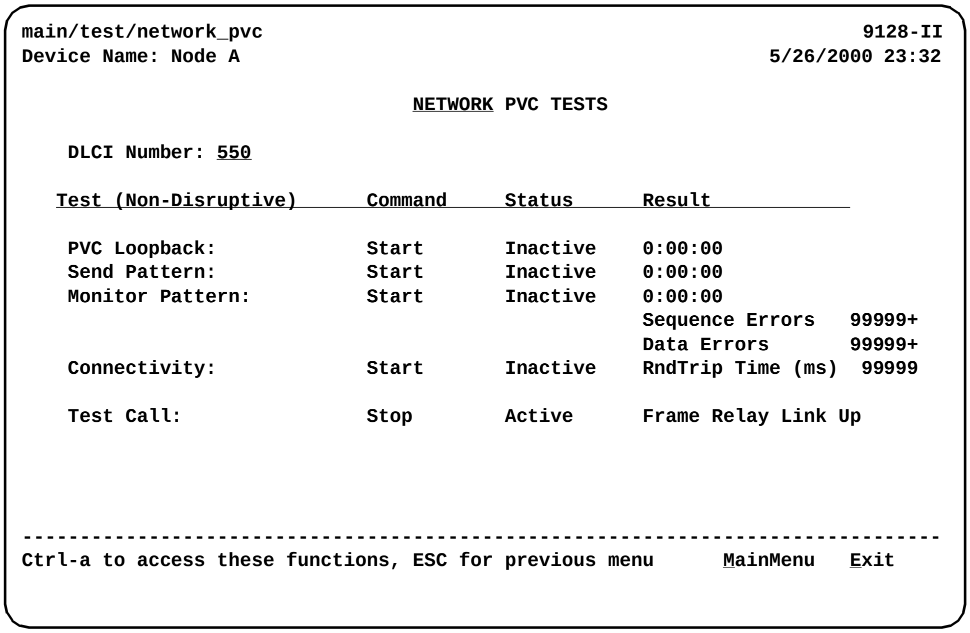
PVC tests can be run on a requested DLCI for a selected interface.

- When PVC tests are on a multiplexed DLCI between FrameSaver devices, they are nondisruptive to data, so user data can continue to be sent during a test.
- If the device at one end of the circuit is not a FrameSaver device, PVC tests are on a standard DLCI and are disruptive to data. Also, the Connectivity test would not appear.

Loopback, and send/monitor pattern tests are available for each interface on the selected DLCI. FrameSaver devices should be at each end of the circuit. If a PVC Loopback is started at one end of the circuit, the other end can send and monitor pattern tests.

The example below shows a PVC Test screen for a FrameSaver unit with ISDN backup capability, with the multiplexed DLCI 550 selected. If a standard DLCI was selected, **`(Disruptive)`**, rather than **`(Non-Disruptive)`**, would be displayed after Test. Also, the Connectivity test would not appear.

PVC Tests Screen Example



```
main/test/network_pvc                                                  9128-II
Device Name: Node A                                           5/26/2000 23:32

                                 NETWORK PVC TESTS

    DLCI Number: 550

   Test (Non-Disruptive)      Command     Status      Result

    PVC Loopback:             Start       Inactive    0:00:00
    Send Pattern:             Start       Inactive    0:00:00
    Monitor Pattern:          Start       Inactive    0:00:00
                                                      Sequence Errors   99999+
                                                      Data Errors       99999+
    Connectivity:             Start       Inactive    RndTrip Time (ms)  99999

    Test Call:                Stop        Active      Frame Relay Link Up




--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

If the unit does not have the ISDN DBM feature, or if the ISDN Link Profile’s Link Status is disabled, **`Test Call`** does not appear. An Outbound Phone Number must be configured for **`Test Call`** to appear.

NOTE:

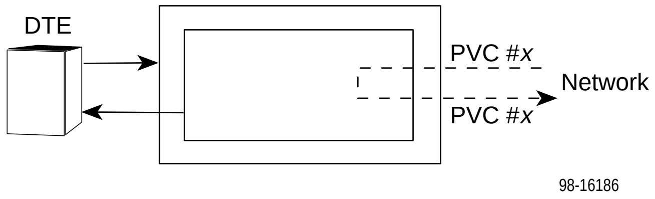
Errors encountered during these tests may be caused by mismatched CIRs in the two FrameSaver units. If errors are detected, verify the CIR configuration and retest.

PVC Loopback

The PVC Loopback loops frames back to the selected interface on a per-PVC basis. This test logically (not physically) loops back frames received from another FrameSaver device through the selected frame relay PVC to the same device.

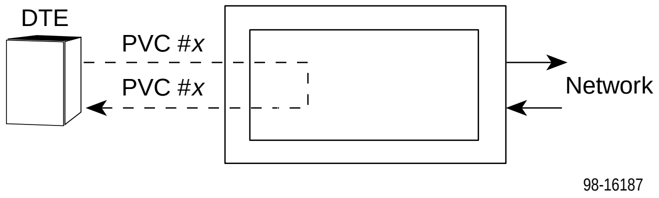
Main Menu→Test→Network PVC Test

Network PVC Loopback



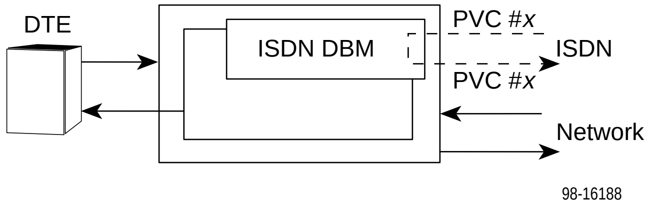
Main Menu→Test→Data Port PVC Tests

Port PVC Loopback



Main Menu→Test→ISDN Call/PVC Tests

ISDN PVC Loopback



Send Pattern

This test sends packets filled with a hexadecimal 55 test pattern and sequence number over the selected interface and DLCI to another FrameSaver device.

To send a pattern test on a link:

*Main Menu→Test→[Network PVC Tests/Data Port PVC Tests/
ISDN Call/PVC Tests]*

If the selected DLCI is configured as . . .	Then . . .	And the default Rate (Kbps) setting is . . .
Standard	**`(Disruptive)`** appears after Test	100% of CIR
Multiplexed	**`(Non-Disruptive)`** appears after Test	10% of CIR

If the CIR is zero, the pattern will be sent at a rate of 1000 bps.

Monitor Pattern

This test monitors packets filled with a hexadecimal 55 test pattern and sequence number over the selected interface and DLCI to another FrameSaver device.

To monitor a pattern test on a link:

*Main Menu→Test→[Network PVC Tests/Data Port PVC Tests/
ISDN Call/PVC Tests]*

The current number of sequence and data errors are shown under the Result column when the FrameSaver unit is in sync. An **`Out of Sync`** message appears when 5 frames out of 25 are missing or out of sequence.

These error counts are updated every second. If the maximum count is reached, **`99999+`** appears in these fields.

Connectivity

Connectivity is a proprietary method that determines whether the FrameSaver device at the other end of the frame relay PVC is active. This test stops automatically and can only be executed for circuit multiplexed PVCs.

To run a connectivity test on a link:

Main Menu→Test→[Network PVC Tests/Data Port PVC Tests/
ISDN Call/PVC Tests]

Selecting Connectivity sends a frame to the FrameSaver unit at the other end of the PVC. A **`RndTrip Time(ms)`** message appears in the Result column when a response is received within 5 seconds, indicating that the FrameSaver unit at the remote end is alive (operational and connected), and the round trip (RT) time is shown in milliseconds (ms), with a resolution of 1 ms. If a response is not received within 5 seconds, **`No Response`** appears in the Result column.

Test Call

Test Call tests the device's ability to place a call. It allows an alternate means of controlling the activation or deactivation of an ISDN link. This test only appears for a FrameSaver device with a DBM that is configured to originate backup calls (typically, the remote site) and has its ISDN Link Status option set to Auto.

To place a test call:

Main Menu→Test→ISDN Call/PVC Tests

When a test call is started, **`Active`** appears in the Status column. While the call is Active, the status of the call connection and the link appears in the Results column.

- A **`Frame Relay Link Up`** message indicates that the required calls have been made and the link is successfully passing LMI data.
- A **`Frame Relay Link Suboptimal`** message indicates that at least one call has been made on the link, the link is successfully passing LMI data, but the Maximum Link Rate configured in the ISDN Link Profile has not been achieved for the link.
- A **`Frame Relay Link Down`** message indicates that the call attempts were not successful.

NOTE:

Primary network data is not affected by a test call. If there is a network failure while a test call is active, the test call is terminated and the call is automatically converted to a backup call.

Physical Tests

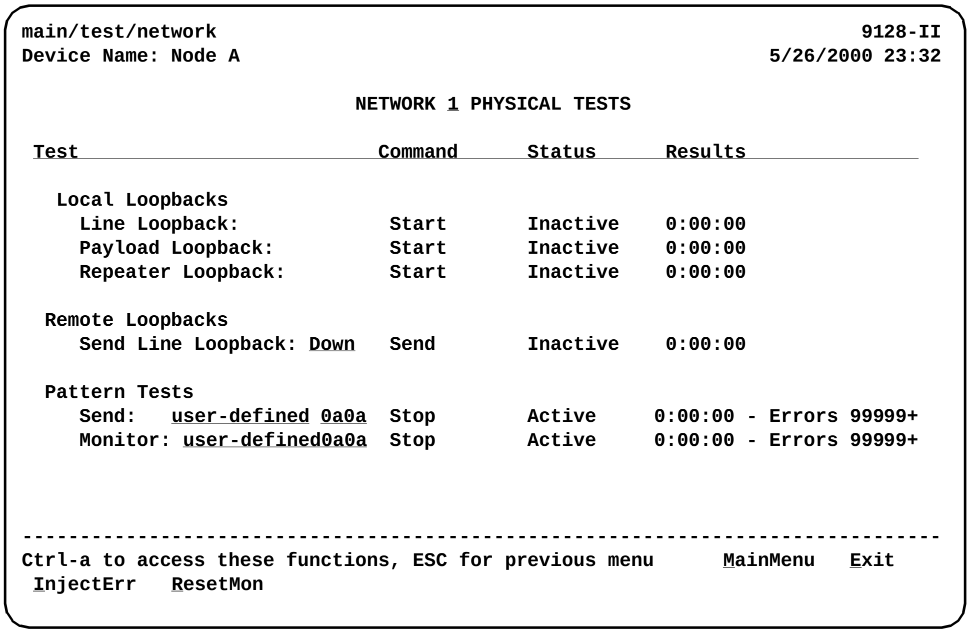
Physical tests require the participation of your network service provider.

Main Menu→Test→[Network Physical Tests/Data Port Physical Tests/ DSX-1 Physical Tests/PRI Physical Tests]

If the unit does not have the ISDN PRI DBM feature, PRI Physical Tests does not appear.

A FrameSaver unit's physical tests screen for the network interface is shown below.

Physical Tests Screen Example



```
main/test/network                                                     9128-II
Device Name: Node A                                           5/26/2000 23:32

                            NETWORK 1 PHYSICAL TESTS

 Test                          Command      Status      Results

   Local Loopbacks
     Line Loopback:             Start       Inactive    0:00:00
     Payload Loopback:          Start       Inactive    0:00:00
     Repeater Loopback:         Start       Inactive    0:00:00

  Remote Loopbacks
     Send Line Loopback: Down   Send        Inactive    0:00:00

  Pattern Tests
     Send:   user-defined 0a0a  Stop        Active     0:00:00 - Errors 99999+
     Monitor: user-defined0a0a  Stop        Active     0:00:00 - Errors 99999+



--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
 InjectErr   ResetMon
```

The InjectErr function key at the bottom of the screen only appears when a Send Pattern Test is Active. Select InjectErr to inject a single bit error into the pattern being sent.

The ResetMon function key at the bottom of the screen only appears when a Monitor 511 test pattern is Active. Select ResetMon to reset the monitor pattern error counter.

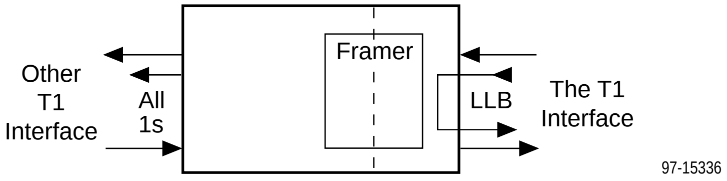
CAUTION:

You should not run these tests with frame relay equipment attached; you must disconnect the frame relay equipment and use external test equipment.

Line Loopback

The Line Loopback (LLB) loops the information received on the selected interface back to the source of the loopback. When used with a pattern test at the remote node, LLB determines whether the problem is with the sending device or the T1 facility.

Main Menu→Test→Network Physical Tests



CAUTION:

This test may affect operation of frame relay PVCs assigned to the selected port. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

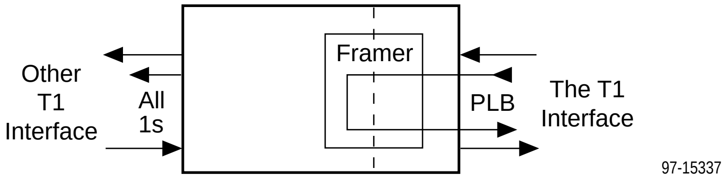
An LLB cannot be started when one of the following tests is active:

- Payload Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- Repeater Loopback on any other T1 interface with DS0s assigned to this network interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) assigned to this network interface.

Payload Loopback

The Payload Loopback (PLB) loops the information received on the selected interface back to the network after it has passed through the receive and transmit framing section of the device. Use the PLB to determine whether the problem is with the T1 facility or in the circuitry of the remote device.

Main Menu→Test→Network Physical Tests



CAUTION:

This test may affect operation of frame relay PVCs assigned to the selected interface. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

A PLB cannot be started when one of the following tests is active:

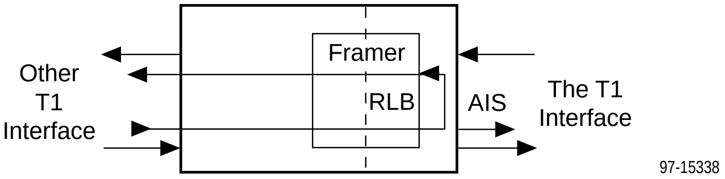
- Line Loopback, Repeater Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- Payload or Repeater Loopback on any other T1 interface with DS0s assigned to this network interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.

Repeater Loopback

The Repeater Loopback (RLB) loops data received from the data ports and the DSX-1 interface after the signal has passed through the framing circuitry. Use RLB to ensure that all of the data is correct up to the point where it is sent over the interface. This helps to indicate that the FrameSaver unit is operational.

Main Menu→Test→Network Physical Tests

An attached device or test equipment should generate and monitor data to be looped back.



The FrameSaver unit will not respond to any messages from the network during this test.

CAUTION:

This test may affect operation of frame relay PVCs assigned to the selected interface. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

An RLB cannot be started when one of the following tests is active:

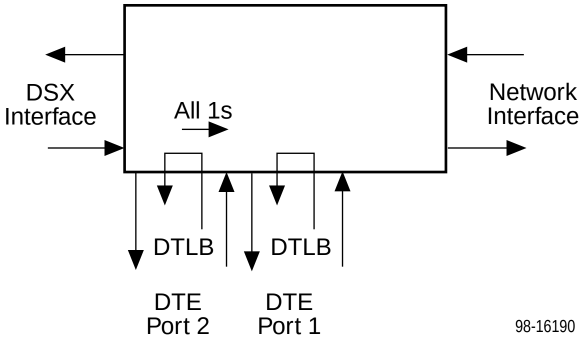
- Payload Loopback, Send Remote Line Loopback, or an active Monitor Pattern on this network interface.
- All loopbacks on any other T1 interface with DS0s assigned to this network interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) assigned to this network interface.

DTE Loopback

The DTE external Loopback (DTLB) test loops the received signal on a DTE interface back to the DTE without affecting the operation of the remaining ports. Use this test for isolating problems on the DTE interface.

Main Menu→Test→Data Port Physical Tests

An attached device or test equipment must generate data to be looped back.



CAUTION:

This test may affect operation of frame relay PVCs assigned to the selected port. Any IP data being sent while this test is active will be disrupted.

Send Line Loopback

The remote Line Loopback (LLB) up and down codes are in-band codes that allow control of a remote device. The LLB Up code invokes a line loopback in the remote unit while the LLB Down code terminates the remote line loopback. Network loopbacks are defined in AT&T TR 62411.

A remote LLB cannot be started when one of the following tests is active:

- Any Loopback on the same interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.
- Data Channel Loopback on the frame relay link on this network interface.

▶ Procedure

To start and stop a Line Loopback:

1. Follow this menu selection sequence:

   Main Menu→Test→Network Physical Tests

2. Select the **Up** code in the Send Line Loopback row to put a remote device in loopback.
3. To start the test, highlight **Send** under Command in the Send Line Loopback row and press Enter. The code is sent for up to 10 seconds, or until an acknowledgement is received from the remote end. The length of time that the test has been running is shown in the Results column.
4. To stop the test, send the **Down** code to take the remote device out of loopback.

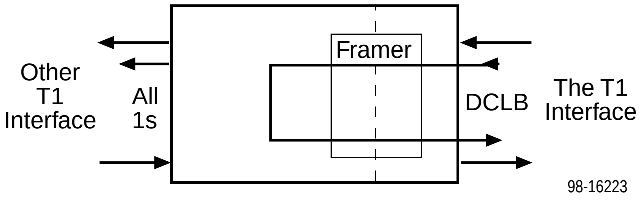
Data Channel Loopbacks on a Frame Relay Link

A network-initiated Data Channel Loopback (DCLB) loops data over the frame relay link (DS0s) received on the network interface through the FrameSaver unit's framing circuitry and back to the same interface.

A DCLB can be controlled over the frame relay link using one of the following in-band methods:

- V.54 Loopback.
- ANSI T1.403 Annex B Fractional T1 (FT1) Channel Loopback.

The frame relay service provider can use DCLB to verify the integrity of the frame relay circuit.



CAUTION:

V.54 and FT1 Loopbacks may affect operation of frame relay PVCs assigned to the selected port. While in loopback, the frame relay link will be down so any IP data being sent while this test is active will be disrupted.

Send Remote Line Loopback

The remote Line Loopback (LLB) up and down codes are in-band codes that allow control of a remote device. The LLB Up code invokes a line loopback in the remote unit while the LLB Down code terminates the remote line loopback. Network loopbacks are defined in AT&T TR 62411.

A remote LLB cannot be started when one of the following tests is active:

- Any Loopback on the same interface.
- Send Pattern Test on this network interface or any synchronous data port (Port Use set to Synchronous) assigned to this interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.
- Data Channel Loopback on the frame relay link on this network interface.

▶ Procedure

To start and stop a Remote Line Loopback:

1. Follow this menu selection sequence:

   Main Menu→Test→[Network Physical Tests/PRI Physical Tests]

2. Select the desired network interface (shown in the screen title).
3. Select the **Up** code in the Remote Line Loopback row to put a remote device into loopback.
4. To start the test, highlight **Send** under Command in the Remote Line Loopback row and press Enter. The code is sent for up to 10 seconds, or until an acknowledgement is received from the remote end. The length of time that the test has been running is shown in the Results column.
5. To stop the test, send the **Down** code to take the remote device out of loopback.

Send and Monitor Pattern Tests

The pattern tests enable a FrameSaver unit to either send or monitor a known bit pattern. These tests generate industry-standard bit patterns that can be used to determine whether information is being correctly transmitted across a circuit.

The following test patterns are available:

- — QRSS
- — All-zeros
- — All-ones
- — 1-in-8
- — 3-in-24
- — 63
- — 511
- — 2047
- — 2E15-1 (2^{15}-1)
- — 2E20-1 (2^{20}-1)
- — User-defined 2-byte test pattern (a0a0)

A Send Pattern test cannot be started when the following tests are running:

- Any Loopback on the same interface.
- Send Pattern Test on any port assigned to this network interface.
- Send V.54 or FT1 Loopback, or Data Channel Loopback on any synchronous data port (Port Use set to Synchronous) and assigned to this network interface.

▶ Procedure

To send and monitor a Pattern Test:

1. Follow this menu selection sequence:

   Main Menu→Test→[Network Physical Tests/DSX-1 Physical Tests]

2. Select the desired pattern in the Send or Monitor field. If sending/monitoring a user-defined pattern, enter the the desired 2-byte hexadecimal value in the field next to Send or Monitor.

   When sending a pattern, the InjectERR function key appears. Use InjectERR if you want to inject a bit error in the transmitted bit pattern.

3. To send a pattern, highlight the **Send** command to send a pattern and press Enter.

   To monitor the test, highlight the **Start** command and press Enter.

   The length of time that the test has been running is shown in the Result column. An error count is also displayed. When monitoring a pattern, the ResetMon function key appears. ResetMon resets the error count to zero.

4. To stop the test, press Enter to send the **Stop** command. **Start** reappears and the status of the test changes back to **Inactive**.

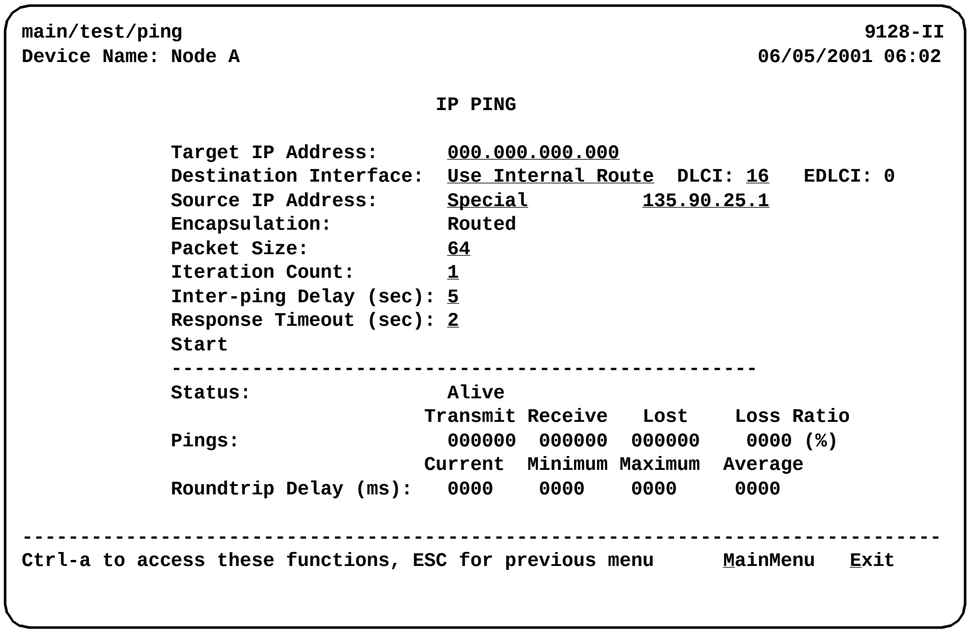
IP Ping Test

An IP Ping test can be run to test connectivity between the FrameSaver unit and any FrameSaver unit, router, or NMS to which it has a route.

Times when you might want to run an IP Ping test are:

- To test connectivity between the FrameSaver unit and any FrameSaver unit in the network to verify that the path is operational. Select *IP Ping Test – Procedure 1* on page 8-39 to ping any far-end FrameSaver unit.
- To verify the entire path between a newly installed remote site FrameSaver unit and the central site NMS. During a remote-site installation, an IP Ping test is typically run from the remote site to ping the NMS at the central site. The remote FrameSaver unit must have SNMP trap managers configured, and one of those trap managers must be the central site NMS. Select *IP Ping Test – Procedure 2* on page 8-40 to ping the NMS at the central site.
- To test the path to the NMS trap managers during installation of the central site FrameSaver unit. The remote FrameSaver unit must have configured the SNMP trap managers to be sent the ping. Select *IP Ping Test – Procedure 2* on page 8-40 to ping SNMP trap managers.

Ping Screen Example



```
main/test/ping                                                           9128-II
Device Name: Node A                                             06/05/2001 06:02

                                    IP PING

             Target IP Address:      000.000.000.000
             Destination Interface:  Use Internal Route  DLCI: 16   EDLCI: 0
             Source IP Address:      Special          135.90.25.1
             Encapsulation:          Routed
             Packet Size:            64
             Iteration Count:        1
             Inter-ping Delay (sec): 5
             Response Timeout (sec): 2
             Start
             ---------------------------------------------------
             Status:                 Alive
                                   Transmit Receive   Lost    Loss Ratio
             Pings:                  000000  000000  000000    0000 (%)
                                   Current  Minimum Maximum  Average
             Roundtrip Delay (ms):   0000    0000    0000     0000

--------------------------------------------------------------------------------
Ctrl-a to access these functions, ESC for previous menu      MainMenu   Exit
```

Table 8-5. Ping Options (1 of 3)

Target IP Address
Possible Settings: **000.000.000.001–126.000.000.000, 128.000.000.000–223.255.255.255** Default Setting: **000.000.000.000**
Specifies the IP address to which a ping will be sent. **000.000.000.001–126.000.000.000, 128.000.000.000–223.255.255.255** – Specifies the IP address.
Destination Interface
Possible Settings: **Use_Internal_Route, Port-*n*, Net1-FR1** Default Setting: **Use_Internal_Route**
Specifies the routing method or destination interface for the ping. **Use_Internal_Route** – When choosing which interface to send the ping, the unit first consults its routing table. If the address or subnet does not appear in the routing table, the ping will be sent to the Default IP Destination, if defined. (See *Configuring Node IP Information* in Chapter 4, *Configuration Options*.) **Port-*n*, Net1-FR1** – The ping is sent out the specified destination regardless of the internal route configuration.
DLCI
Possible Settings: **16–1007** Default Setting: [Lowest assigned DLCI on the selected interface]
Specifies the DLCI to be used for the ping. If the DLCI is configured on a Virtual Channel Connection (VCC), the VCI and VPI are displayed next to the DLCI. *Display Conditions* – This setting does not appear when Destination Interface is set to Use_Internal_Route. **16–1007** – Specifies the DLCI.
EDLCI
Possible Settings: **0** Default Setting: **0**
Specifies the EDLCI to be used for the ping. *Display Conditions* – This setting does not appear when Destination Interface is set to Use_Internal_Route, and then appears only if the specified DLCI is multiplexed. **0** – Specifies the EDLCI. The field cannot be modified.

Table 8-5. Ping Options (2 of 3)

Source IP Address
Available Settings: **Automatic, Special** Default Setting: **Automatic**
Specifies the source IP address to be identified with the ping. *Display Conditions* – This setting does not appear when Destination Interface is set to Use_Internal_Route. **Automatic** – The source IP address is: – The interface IP address, if one exists, else – The node IP address if one exists, else – The first available address in the address table **Special** – The entered IP address is shown as the source. When Special is specified, and additional field is displayed that allows you to enter an IP address 000.000.000.001–126.255.255.255, or 128.000.000.000–223.255.255.255.
Encapsulation
Available Settings: **Routed** Default Setting: **Routed**
Specifies the IP encapsulation used by the data stream. This read-only field specifies that the IP encapsulation used is RFC 1490/RFC 2427 routed Network Level Protocol IDentifier (NLPID) encapsulation, and not SubNetwork Attachment Point (SNAP) encapsulation. *Display Conditions* – This setting does not appear when Destination Interface is set to Use_Internal_Route. **Routed** – The encapsulation is routed NLPID.
Packet Size
Available Settings: **36–4096** Default Setting: **100**
Specifies the size of the ping packet including the IP header (20 bytes) and the ICMP header (8 bytes). **1–4096** – Packet size.
Iteration Count
Available Settings: **1–999999** Default Setting: **5**
Specifies the number of pings to send. **1–999999** – Number of pings.
Inter-Ping Delay
Available Settings: **1–900** Default Setting: **1**
Specifies, in seconds, the amount of time to wait between pings. **1–900** – The ping wait time.

Table 8-5. Ping Options (3 of 3)

Response Timeout
Available Settings: **1–60** Default Setting: **2**
Specifies the amount of time, in seconds, to wait before a host that has not responded to a ping is declared unreachable. **1–60** – The response timeout period.

When the ping has completed normally, timed out, or been stopped using the Stop command, informational fields are displayed as shown in Table 8-6, Ping Responses.

Table 8-6. Ping Responses

Field	Possible Values	Description
Status	■ In Progress ■ Alive ■ Destination Unreachable ■ Ping Timed Out ■ No route in this device	■ Ping has been sent. ■ Ping was successful. ■ The host could not be reached. See RFC 792 for possible causes. ■ There was no response in the period specified in Response Timeout. ■ The IP address is not in the routing table, and no Default IP Destination is configured.
Ping Loss Ratio (%)	0–100	The ratio of pings received to pings transmitted.
Pings Transmitted	1–999999	The number of pings transmitted.
Pings Received	1–999999	The number of pings received.
Pings Lost	1–999999	The number of pings transmitted less the number of pings received.
Current Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The time in milliseconds that it took to complete the latest ping.
Minimum Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The least time in milliseconds that it took to complete a ping during this test.
Maximum Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The most time in milliseconds that it took to complete a ping during this test.
Average Roundtrip Delay	■ 0 ■ 1–9999	■ No measurement exists. ■ The average time in milliseconds that it took to complete a ping during this test.

IP Ping Test – Procedure 1

▶ Procedure

To ping any far-end FrameSaver unit:

1. Select the IP Ping test.

   Main Menu→Test→IP Ping

2. Enter the IP Address of the device the ping is being sent to, then select Start.

   NOTE:

   If the FrameSaver unit has just initialized, or the far-end unit has just initialized, it may take about a minute for the units to learn the routes via the proprietary RIP.

3. Verify the results of the IP Ping test.

   — While the test is running, **`In Progress...`** appears in the Status field.

   — When the test is finished, **`Alive`** should appear as the Status. If any other message is displayed, additional testing is required.

IP Ping Test – Procedure 2

▶ **Procedure**

To ping the NMS at the central site:

1. Verify that the central site NMS has the FrameSaver unit's IP address in its routing table so it can communicate with the FrameSaver unit.

2. Verify that the central site NMS's router has the FrameSaver unit's IP address in its routing table so it can communicate with the FrameSaver unit.

3. Verify that the central site NMS has been configured as an SNMP Trap Manager if the router is to route data, so a route has been configured within the FrameSaver unit.

   Main Menu→Configuration→Management and Communication→ SNMP Traps

   Or, for a local DLCI between the central site FrameSaver unit and its router, verify that a Default IP Destination route has been configured.

   Main Menu→Configuration→Management and Communication→ Node IP→*Default IP Destination*

   Configure both SNMP Traps and a Default IP Destination when PVC Multiplexing is used, as when using the Auto-Configuration feature.

4. Select the IP Ping test.

   Main Menu→Test→IP Ping

5. Enter the IP Address of the central site NMS, then select Start.

6. Verify the results of the IP Ping test.

   — While the test is running, **`In Progress...`** appears in the Status field.

   — When the test is finished, **`Alive`** should appear as the Status. If any other message is displayed, additional testing is required.

Lamp Test

The FrameSaver unit supports a Lamp Test to verify that all LEDs are lighting and functioning properly. All LEDs flash or blink on and off at the same time every 1/2 second during execution of the test. When the test is stopped, the LEDs are restored to their normal condition.

Main Menu→Test→Lamp Test

If the Test Timeout configuration option is enabled and a Test Duration is set, the Lamp Test stops when the test duration expires. See *Test Timeout Feature* on page 8-19*,* for additional information.

Setting Up OpenLane for FrameSaver Devices and Activating SLM Features

9

This chapter includes:

OpenLane Support of FrameSaver Devices

The OpenLane Service Level Management (SLM) system provides the following features:

- Web and database services
- Web access to health and status information
- Web access to real-time, as well as historical graphs and reports
- Web access to SLV reports, for units with the SLM feature set activated
- On-demand polling of FrameSaver devices
- SNMP polling and reporting
- Web-based diagnostic tests: end-to-end, PVC loopbacks, connectivity, and physical interface tests
- Basic device configuration, including RMON alarm and threshold configuration when the unit has the advanced SLM feature set activated
- Automatic device and PVC discovery for SLM devices with their SLV Delivery Ratio configuration option enabled
- Easy firmware downloads to an entire network or parts of the network
- Remote SLM feature activation for units with the diagnostic feature set
- Multiple maintenance schedules for scheduling more than one maintenance period, with a report for each scheduled task
- Multiple Circuit IDs for multiple access levels so customers, as well as network service providers, have access to network management information
- Device reset capability
- HP OpenView adapters for integrating OpenLane with the OpenView Web interface

Setting Up the OpenLane SLM System

Instructions for installing the OpenLane SLM system are found in the *Product-Related Documents*.

In addition to installation instructions, the Administrator's Guide contains instructions for:

- Starting and stopping the OpenLane Web and database services
- Accessing the OpenLane application
- Adding a FrameSaver device
- Adding a Customer ID

OpenLane SLM also has an extensive online Help system.

Setting Up FrameSaver Support

With OpenLane SLM's extensive online Help, the application is self-documenting and you have access to the most current system information.

▶ Procedure

To set up FrameSaver support:

1. Start the OpenLane services, then access the application.
2. Log in as **Admin** for access to customer profiles, frame relay access facilities components, and PVC components.
3. Add FrameSaver devices.
4. Create customer profiles.
5. Set up historical data collection.
6. Set up SLV report filters for Web access to report data for FrameSaver devices with the SLM feature set activated.

See the *Product-Related Documents* and OpenLane online Help to learn how to perform these steps and for additional information.

Ordering SLM Feature Set Activations

When advanced SLM functionality is needed at a site, an Activation Certificate (Feature No.9126-C1-220 or 9128-C1-220) can be ordered, which will allow you to activate SLM features in FrameSaver devices with the diagnostic feature set. You must have the OpenLane SLM system, Release 5.3 or later, to activate SLM capability in FrameSaver devices and to manage your certificates.

NOTE:

If you have a combination of models in your network, a separate Activation Certificate must be ordered for each model number. Each certificate can be ordered for a single unit or for many units.

Contact one of the following to request an Activation Certificate:

- If you are an end user and managing your own network, contact your sales representative or distributor.
- If your network service provider (NSP) manages the network, contact the service provider.
- If you are a network service provider or distributor, contact Paradyne at 1-800-727-2396, **www.paradyne.com**, via a purchase order, or your Electronic Data Interchange (EDI). If submitting a purchase order by fax, send it to 1-727-532-5270.

  An Activation Certificate can also be ordered through the Paradyne store at **www.paradyne.com/store**.

Provide the following information:

- Model (9126 or 9128)
- Number of units to be activated
- Your OpenLane SLM system license key number

To Find Your License Key Number

Your license key number was entered into your system when your OpenLane SLM system was installed and is available from the OpenLane Administration screen. However, to access the screen with your license key number, you must log in as a user with Administrative system access.

▶ Procedure

To find your OpenLane license key number:

1. Open the OpenLane SLM application and log in as a user with Administrative access (e.g., **ADMIN**).
2. A bottom of the OpenLane Administration screen, select **`About OpenLane SLM`**.

   The license key is shown mid-screen, below the copyright and build information.

The Activation Certificate

An Activation Certificate will be sent to you via Federal Express.

NOTE:

If you ordered an Activation Certificate via e-mail, Activation Certificate information will be e-mailed to you so you can start activating units immediately. The actual certificate will arrive the next day.

When the certificate arrives, it will include the following information:

- Activation Certificate number
- Your OpenLane License Key number
- Model Prefix (9126 or 9128)
- Feature Group: SLM
- Number of device activations ordered (included on this certificate)
- Sales order number
- Customer purchase order number
- Customer or company name
- Contact (sent to the attention of)
- Shipping address
- Phone number
- E-mail address
- Date the certificate was generated

Administering and Managing SLM Activations

The OpenLane SLM system provides the following features that allow you to administer and manage your Activation Certificates and SLM activations. From the Firmware/Feature Maintenance menu, you can:

- Add or view the status of activations, and see how many activations remain on each certificate.
- Schedule when activations are to take place, and verify that the activations occurred as scheduled.
- View activations that are scheduled, cancel activations, or change the FrameSaver devices that are scheduled for activation, as needed.
- Generate and print a report that summarizes the activity on all Activation Certificates in your system, which includes the number of activations ordered, the number of activations remaining on the certificate, and the date the certificate was ordered.

  The report also includes information about each activated unit: its system name, IP address, location, model, serial number, and date of activation.

The sections that follow describe what you need to do to get Activation Certificate information into your OpenLane SLM system, and to activate SLM capability in units with the diagnostic feature set.

Entering an Activation Certificate

Once you receive an Activation Certificate, enter the Activation Certificate number into your OpenLane SLM system's database.

▶ Procedure

To enter the Activation Certificate number:

1. Open the OpenLane SLM application and provide your access level, which must be **Admin**.
2. Select **`Firmware/Feature Maintenance`** from the OpenLane Administration screen.
3. In the Feature Activations area, select **`View/Add activation certificates,`** located near the bottom of the Firmware/Feature Maintenance menu.
4. If no Activation Certificates have been entered into the system, or if adding another certificate:
   - Click inside the New certificate box under **`Add certificate`**.
   - Enter the Activation Certificate number from the certificate.
   - Click on the prompt below it. The frame at the bottom of the screen is refreshed to display information about the new certificate.

See the OpenLane SLM system's online Help for additional information.

Checking Activation Certificate Status

You can view the status of certificates and activations at any time by selecting **`View/Add activation certificates`** from the Firmware/Feature Maintenance menu, and clicking on the prompt below **`Display certificates`**.

See the OpenLane SLM system's online Help for additional information.

Scheduling Activations

You can activate one, many, or all FrameSaver devices at any time, until all the activations ordered for the certificate have been completed.

NOTE:

Once SLM capability is activated in a FrameSaver device, the unit cannot be returned to the diagnostic feature set.

▶ Procedure

To schedule device activations:

1. Open the OpenLane SLM application and provide your access level, which must be **Admin**, and select **`Firmware/Feature Maintenance`** from the OpenLane Administration screen.
2. In the Feature Activations area, select **`Schedule feature verifications/activations`**.
3. Follow the steps included on this screen.

   — Select the FrameSaver devices to be activated at this time by model, device name, or IP address, and click on the prompt below the selection table.

   Entering an asterisk (*) in the Name or Device IP field will display all FrameSaver devices in your system, so you can pick and choose devices that will be activated.

   — Select whether to activate selected devices.
4. Select the FrameSaver devices to be activated at this time under **`Select devices`** by model, device name, or IP address, then click on the prompt below the device selection table. The table in the lower frame lists all the devices in the selected category.

   Entering an asterisk (*) in the Name or Device IP field will display all FrameSaver devices in your system, so you can pick and choose devices that will be activated.
5. In the lower frame, click on the box in the Activate column to select or deselect a specific FrameSaver device for activation. Proceed through the list until you have selected all the devices to be activated at this time.
6. Proceed through the other steps included on this screen, then click on the prompt under **`Perform the scheduled verification/activation`** to verify what you scheduled. The Verify/Schedule Feature Activations screen appears so you can verify the scheduling information.

   — If the information is correct, click on Apply.

   — If not, or if you want to verify or change the devices that will be activated or the time the activations are to occur, click on the prompt to return to the previous screen and reselect you options.

Checking the Status of Scheduled Activations

You can check the status of scheduled activations or cancel activations at any time prior to the activations taking place by selecting **`View/Abort scheduled task status`** from the Firmware/Feature Maintenance menu. You can select all tasks, or select tasks by model, device name, or IP address. When you click on the prompt below the **`Select tasks`** table, the table in the lower frame lists all the devices in the selected category scheduled for activation.

See the OpenLane SLM system's online Help for additional information.

Canceling Scheduled Activations

To cancel scheduled activations, select **`View/Abort scheduled task status`** from the Firmware/Feature Maintenance menu, select the desired tasks, and click on the prompt to display the FrameSaver devices scheduled for activation.

Click on the box in the Abort column to select the FrameSaver devices that will not be activated, then click on the prompt under **`Abort verifications/activations`** to verify your selections, and Apply. Activations for the selected devices will be cancelled.

See the OpenLane SLM system's online Help for additional information.

Accessing and Printing the Certificate Summary Report

The Certificate Summary Report provides information about the Activation Certificate and the activated devices. Select **`Generate certificate summary report`** from the Firmware/Feature Maintenance menu.

The report lists all Activation Certificates in your OpenLane SLM system and all the FrameSaver devices activated using each certificate.

- Activation Certificate information includes the model, feature, the number of activations ordered, the number of activations still covered by the certificate, and the date the certificate was ordered.
- Device activation information includes the device's name, IP address, its location, model, serial number, and the date the device was activated.

We recommend that you print and save this report. However, before printing change the orientation of the report to Landscape so no information is truncated.

See the OpenLane SLM system's online Help for additional information.

Setting Up NetScout Manager Plus for FrameSaver Devices

10

This chapter includes NetScout Manager Plus information as it relates to FrameSaver SLV devices. It includes the following:

Release 5.5 or higher of the NetScout Manager Plus software provides FrameSaver SLV-specific support.

Preparation

Before getting started, you need to copy some OpenLane directories to a NetScout Manager Plus user directory. OpenLane provides these directories as a starting point for loading new alarms and creating history files. A template of alarms and values for configuring alarms and several templates for creating history files specific to the FrameSaver unit are available.

OpenLane paradyne directories include the following:

- **Properties:**
  `paradyne.fsd` file found in **`OpenLane/netscout/alarms/directory`**
- **Properties:**
  `paradyne.fst` file found in **`OpenLane/netscout/alarms/directory`**
- **Alarms:**
  `slvtemplate.fct` file found in
  `OpenLane/netscout/alarms/directory`
- **User history:**
  `pd*.udh` files found in **`OpenLane/netscout/userHistory/directory`**

These files should be moved to **`$NSHOME/usr`** so they can be used.

See *Adding SLV Alarms Using a Template* on page 10-8 and *Creating History Files* on page 10-13 for additional information.

Configuring NetScout Manager Plus

For the NetScout Manager Plus main window to appear, make sure your environment is set up exactly as specified in your NetScout Readme file. You need to:

- Copy the OpenLane directory to a user directory.
- Add frame relay agents to the NetScout Manager.
- Configure agent properties.
- Verify and correct domains and groups.
- Monitor the agent and DLCIs.

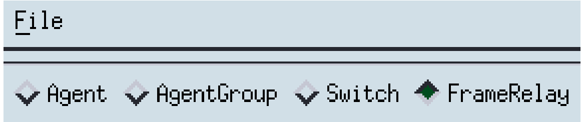
Refer to the NetScout documentation for additional information about accessing and managing the FrameSaver SLV unit through NetScout Manager Plus, refer to the:

- *NetScout Manager/Plus User Guide* to help you install the application, monitor traffic, and diagnose emerging problems on network segments.
- *NetScout Manager/Plus & NetScout Server Administrator Guide* to help you configure agents, remote servers, and report templates using the various NetScout products.
- *NetScout Probe User Guide* to help you install the NetScout Probe between the FrameSaver unit and its router, and configure the probe on network segments you want to monitor.

Adding FrameSaver SLV Units to the NetScout Manager Plus Network

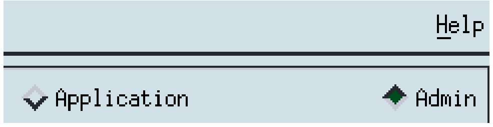
▶ Procedure

1. Bring up the NetScout Manager Plus main window.
2. Select the FrameRelay radio button from the agent type selection bar (on the left side of the window).



   A list of configured frame relay agents appear in the list box below the Name and IP Address headings. If this is a new NetScout Manager Plus installation, the list box below the selection bar is blank since no agents are configured yet.

3. Select the Admin radio button from the application selection bar (to the far right of the screen). Applicable configuration and administration icons appear in the box below the application bar.



4. Click on the Config Manager icon to open the Configuration Manager main window.
5. Select the Add... button (down the center of the screen).
6. Minimally, enter the following:

   — Agent name

   — IP address

   — Enter 1 for the frame relay logical interface to be monitored.

   — Properties File: Select paradyne.

7. Select the OK button at the bottom of the screen to add the agent, discover its DLCIs, and return to the Configuration Manager main window.

   The frame relay agent just entered appears in the agent list box, with its DLCIs in the DLCI list box at the bottom of the screen.

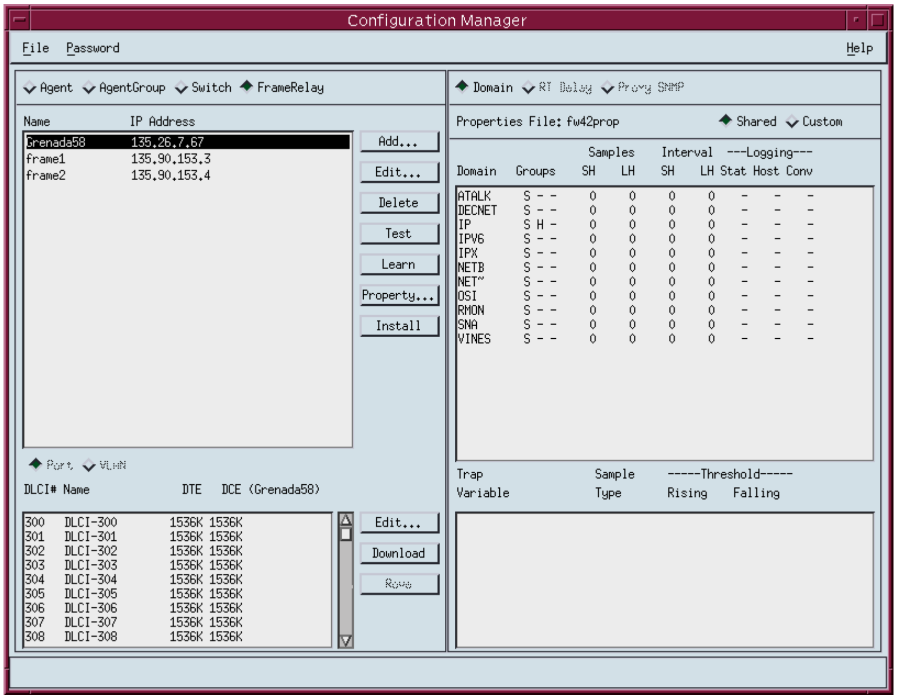
8. Select the Test button (fourth button down, center of the screen) to make sure you can communicate with the agent.

Refer to *Adding Frame Relay Agents* in the *NetScout Manager/Plus & NetScout Server Administrator Guide* for additional information.

Verifying Domains and Groups

▶ Procedure

1. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.



```
Name          IP Address
Grenada58     135.26.7.67
frame1        135.90.153.3
frame2        135.90.153.4
```

```
DLCI# Name          DTE   DCE (Grenada58)
300   DLCI-300      1536K 1536K
301   DLCI-301      1536K 1536K
302   DLCI-302      1536K 1536K
303   DLCI-303      1536K 1536K
304   DLCI-304      1536K 1536K
305   DLCI-305      1536K 1536K
306   DLCI-306      1536K 1536K
307   DLCI-307      1536K 1536K
308   DLCI-308      1536K 1536K
```

Properties File: fw42prop ◆ Shared ◇ Custom

```
                   Samples    Interval   ---Logging---
Domain   Groups    SH    LH   SH    LH  Stat Host Conv
ATALK    S - -     0     0    0     0    -    -    -
DECNET   S - -     0     0    0     0    -    -    -
IP       S H -     0     0    0     0    -    -    -
IPV6     S - -     0     0    0     0    -    -    -
IPX      S - -     0     0    0     0    -    -    -
NETB     S - -     0     0    0     0    -    -    -
NET~     S - -     0     0    0     0    -    -    -
OSI      S - -     0     0    0     0    -    -    -
RMON     S - -     0     0    0     0    -    -    -
SNA      S - -     0     0    0     0    -    -    -
VINES    S - -     0     0    0     0    -    -    -
```

```
Trap               Sample    -----Threshold-----
Variable           Type      Rising    Falling
```

2. Verify that only FrameSaver SLV-supported domains appear listed in the Domain column. FrameSaver SLV-supported domains include:

— ATALK

— DECNET

— IP

— IPV6

— IPX

— NETB

— NET~

— OSI

— RMON

— SNA

— VINES

— NEWVINES

3. Verify that:

— S (statistics collection) appears for each domain listed in the Group column.

— H (hosts) appears for the IP domain only.

— Dashes occupy all other positions under the Group column.

— Zeros appear under the Samples and Interval SH and LH columns.

— Dashes appear under all Logging columns: Stat, Host, Conv.

4. If all these requirements are met, no further action is required. Close the Configuration Manager window.

   If all these requirements are not met, a FrameSaver SLV-supported domain needs to be added, or if an unsupported domain needs to be deleted, the Properties File must be edited.

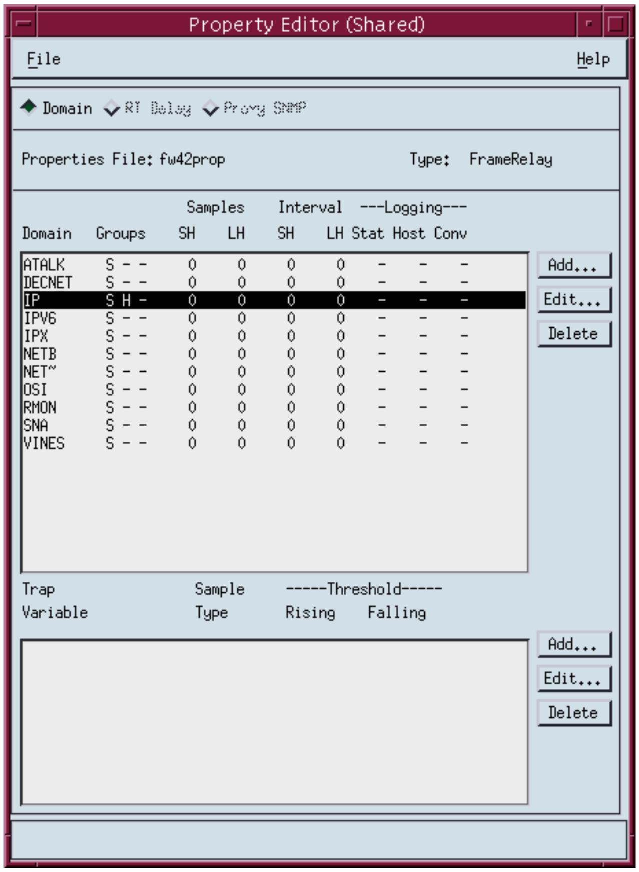
Correcting Domains and Groups

Properties need to be edited when not using the Paradyne-provided file and when:

- An unsupported domain needs to be deleted.
- A missing domain needs to be added.
- Groups, Samples, Interval, and Logging are not configured as specified in Step 3 of *Verifying Domains and Groups*.

▶ Procedure

1. Select the Property... button (down the center of the Configuration Manager main window). The Property Editor window opens.



Properties File: fw42prop

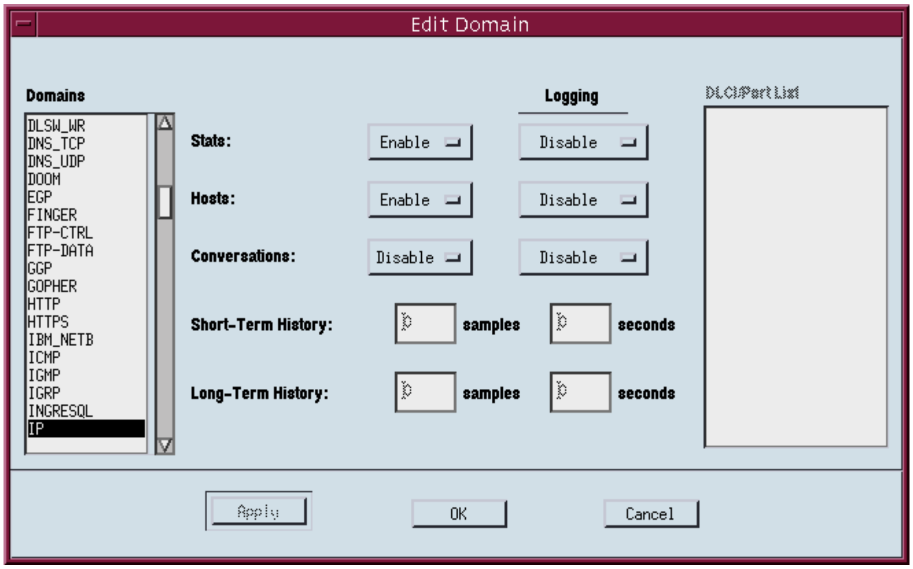
Type: FrameRelay

		Samples		Interval		---Logging---		
Domain	Groups	SH	LH	SH	LH	Stat	Host	Conv
ATALK	S - -	0	0	0	0	-	-	-
DECNET	S - -	0	0	0	0	-	-	-
IP	S H -	0	0	0	0	-	-	-
IPV6	S - -	0	0	0	0	-	-	-
IPX	S - -	0	0	0	0	-	-	-
NETB	S - -	0	0	0	0	-	-	-
NET~	S - -	0	0	0	0	-	-	-
OSI	S - -	0	0	0	0	-	-	-
RMON	S - -	0	0	0	0	-	-	-
SNA	S - -	0	0	0	0	-	-	-
VINES	S - -	0	0	0	0	-	-	-

2. To delete an unsupported domain, click on the domain from the Domains list, then select the Delete button.

   The **`Are you sure?`** prompt appears. Select Yes. The unsupported domain disappears from the list.

3. To add a FrameSaver SLV-supported domain or correct property settings, select the Edit... button (to the right of the Domain section of the Property Editor window). The Edit Domain window opens.



Stats: Enable Disable

Hosts: Enable Disable

Conversations: Disable Disable

Short-Term History: samples seconds

Long-Term History: samples seconds

4. Click on the domain from the Domains list and configure the following:

Property		Description	Setting
Groups	Stats (S)	Statistics collection	Enabled for all domains.
	Hosts (H)	Level 3 information (network)	Enabled for IP domain only. Disabled for all other domains.
	Conversations (C)	Protocols being used	Disabled for all domains.
Logging		Event logging	Disabled for all domains and groups.

5. Select the OK button (at the bottom of the screen) to apply the changes.

Refer to *Configuring Domains in Properties Files* in the *NetScout Manager/Plus & NetScout Server Administrator Guide* for additional information.

Adding SLV Alarms Using a Template

Once DLCIs have been discovered, SLV alarms should be configured and assigned to each DLCI. OpenLane provides a template for configuring alarms. DLCI alarms can be configured manually, but using the Paradyne alarm defaults template greatly reduces configuration time.

The following alarms are configured for each DLCI included in the Paradyne MIB:

- Frames Sent (SLVFramesSnt)
- Tx CIR Utilization (SLVTxCIRUtil)
- Tx DLCI Utilization (SLVTxDLCIUtil)
- Frames Received (SLVFramesRec)
- Rx DLCI Utilization (SLVrxDLCIUtil)
- Frames Sent Above CIR (SLVFramesTxAbvCIR)
- Average Latency (AverageLatency)
- Current Latency (CurrentLatency)

These alarms and current values can be found in $NSHOME/usr/slvtemplate.fct, which is used as a starting point for loading new alarms. This file can be copied and edited so the alarm threshold values match service level agreement values. The copied .fct file can then be used to replicate alarm threshold values for all DLCIs on the unit using the eztrap utility. All .fct files must be in $NSHOME/usr.

To configure alarms manually, see *Adding SLV Alarms Manually* on page 10-11.

NOTE:

Perl must be installed in your system to use the eztrap utility in the procedure below. If you have an NT system, please install Perl before proceeding.

▶ Procedure

1. Open a terminal window and go to **$NSHOME/usr**.
2. Type **eztrap -i** *filename***.fct -o** *agentname***.fct** *agentname* and press Enter to run the eztrap utility to create alarm threshold values across all DLCIs for the copied .fct file.

   The message **`eztrap done`** appears when the .fct file is transferred.
3. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.
4. Edit any alarm values that need to be changed.
5. Select the Install button (down the center of the Configuration Manager main window) to load alarms for the unit. This may take some time, so please be patient.

See *Editing Alarms* on page 10-9 if any default settings need to be changed.

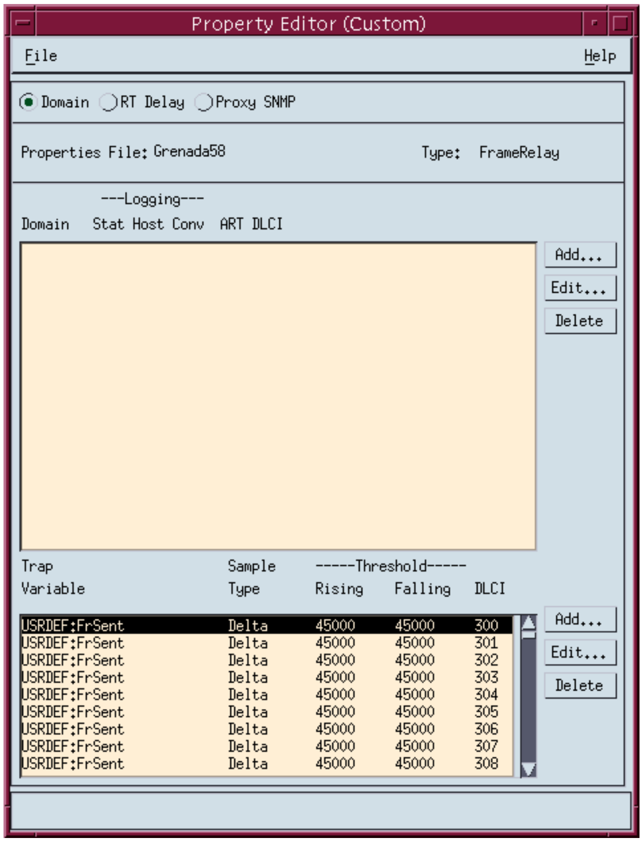
Editing Alarms

▶ Procedure

1. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.

2. Select the Custom radio button from the Properties File area (in the upper right of the window), then Property... (down the center of the screen).

   The Custom Property Editor window opens.



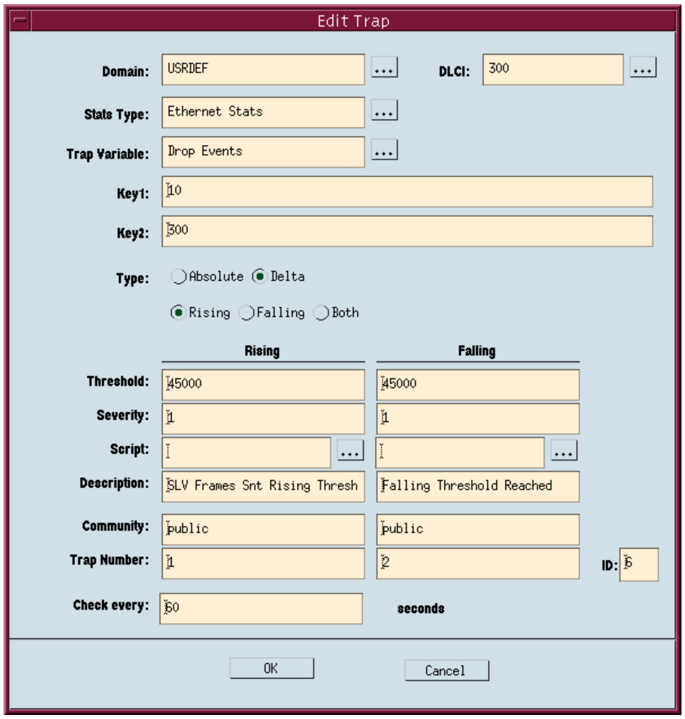
Properties File: Grenada58

Type: FrameRelay

Trap Variable	Sample Type	-----Threshold----- Rising	Falling	DLCI
USRDEF:FrSent	Delta	45000	45000	300
USRDEF:FrSent	Delta	45000	45000	301
USRDEF:FrSent	Delta	45000	45000	302
USRDEF:FrSent	Delta	45000	45000	303
USRDEF:FrSent	Delta	45000	45000	304
USRDEF:FrSent	Delta	45000	45000	305
USRDEF:FrSent	Delta	45000	45000	306
USRDEF:FrSent	Delta	45000	45000	307
USRDEF:FrSent	Delta	45000	45000	308

3. Select a DLCI from the Trap list, and select the Edit... button (to the right of the list).

   The Edit Trap window opens.



Domain: USRDEF ... DLCI: 300 ...

Stats Type: Ethernet Stats ...

Trap Variable: Drop Events ...

Key1: 10

Key2: 300

Type: ○ Absolute ● Delta

● Rising ○ Falling ○ Both

	Rising	Falling
Threshold:	45000	45000
Severity:	1	1
Script:	...	...
Description:	SLV Frames Snt Rising Thresh	Falling Threshold Reached
Community:	public	public
Trap Number:	1	2

ID: 6

Check every: 60 seconds

4. Edit any trap defaults that may be required. See Step 4 on page 10-12 of *Adding SLV Alarms Manually* for field settings you may want to change.

5. Select the OK button (at the bottom of the screen) to apply your changes. The window closes and the Configuration Manager main window reappears.

6. Select the Install button (down the center of the Configuration Manager main window) to apply your changes.

Refer to *Editing Alarms* in the *NetScout Manager/Plus & NetScout Server Administrator Guide* to change alarm thresholds.

Adding SLV Alarms Manually

Once DLCIs have been discovered, SLV alarms should be defined and assigned to each DLCI.

When configuring alarms manually, every alarm must be configured for each DLCI; that is, if there are eight alarms and 20 DLCIs, 160 trap configurations must be created (8 x 20). For this reason, it is recommended that the OpenLane defaults be used. Follow the procedure below to configure alarms manually.

To load OpenLane default settings for alarms, see *Adding SLV Alarms Using a Template* on page 10-8.

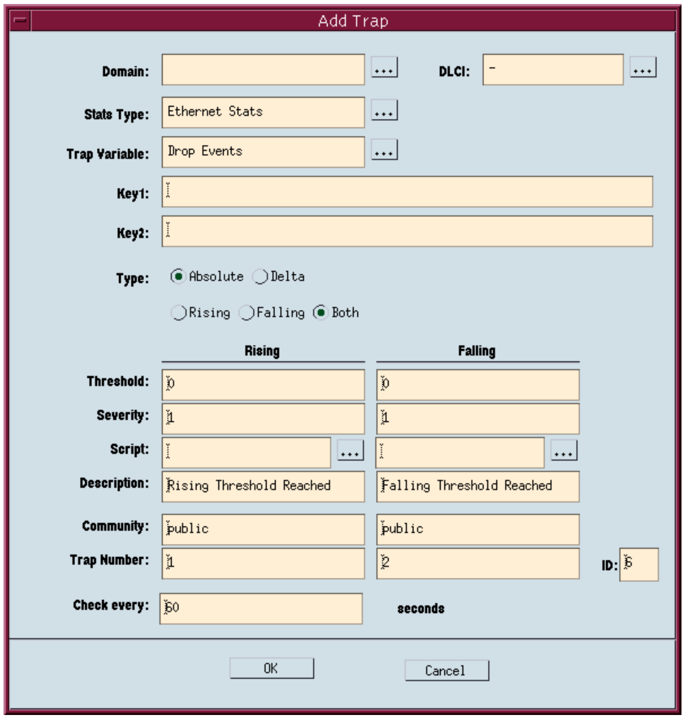
▶ Procedure

1. From the NetScout Manager Plus main window, with the FrameRelay and Admin radio buttons still selected, click on the Config Manager icon to open the Configuration Manager main window.

2. Select the Custom radio button from the Properties File area (in the upper right of the window), then Property... (down the center of the screen).

   The Custom Property Editor window opens (see the window in *Editing Alarms* on page 10-9).

3. Select a DLCI from the Trap list, and select the Add... button (to the right of the list). The Add Trap window opens.



Domain: ... DLCI: – ...

Stats Type: Ethernet Stats ...

Trap Variable: Drop Events ...

Key1:

Key2:

Type: ● Absolute ○ Delta

○ Rising ○ Falling ● Both

	Rising	Falling
Threshold:	0	0
Severity:	1	1
Script:	...	...
Description:	Rising Threshold Reached	Falling Threshold Reached
Community:	public	public
Trap Number:	1	2

ID: 6

Check every: 60 seconds

4. Click on the ... button to the right of indicated fields for a drop-down list from which selections can be made. Minimally, configure the following fields:

Field	**Select or Enter . . .**
Domain	User Defined
DLCI	DLCI number for trap being assigned
Stats Type	PARADYNE
Trap Variable	Trap variable to be configured
Key1	The ifIndex for the frame relay logical interface is 1
Key2	DLCI number (same as DLCI above)
Type	Absolute or Delta radio button* Rising, Falling, or Both radio button**
Threshold	Value that will trigger a trap.

* Latency MIB variables should be Absolute; all others should be Delta.

** Generally, Rising is selected.

5. Select the OK button (at the bottom of the screen) to add this alarm.
6. Repeat Step 3 through Step 5 until all traps are configured for all DLCIs.

Refer to *Configuring Alarms in* the *NetScout Manager/Plus & NetScout Server Administrator Guide* for additional information.

Creating History Files

Up to 14 additional user history tables can be created in the FrameSaver unit for each interface. An interface is a specific DLCI or the entire frame relay interface. A table must be created for each DLCI or frame relay link to be monitored. Additional user history tables are created using the command-line prompt in NetScout Manager Plus to load a file that contains the OIDs (Object IDs) to be monitored into the unit.

OpenLane provides several useful examples, including three files containing a complete set of OIDs appropriate to the interface to be monitored: one for a DLCI, one for a frame relay link, and one containing system-type OIDs. Any of these files can be used as a template when creating customized history files specific to the FrameSaver unit.

These files have a **`pdn*.udh`** (user-defined history) format and are found in the **`OpenLane/netscout/userHistory`** directory. The userHistory files should be moved to **`$NSHOME/usr`** so they can be used.

A separate *.udh file must be created and loaded for each DLCI or link that will be monitored before a customized user history table can be loaded. Use a text editor to create these *.udh files by:

- Copying one of the interface-specific files (DLCI or link) and editing it using one of the examples provided as a guide.
- Copying one of the examples provided and editing the extensions to fit the FrameSaver unit.

CAUTION:

Two user history table files are already configured and installed in the unit, UserHistory1 and UserHistory2. These files must not be modified. These two tables are used to keep SLV data for reports.

It is always a good idea to rediscover agents and their DLCIs before starting to be sure your agent and DLCI lists are current. To rediscover agents and their DLCIs, select the Learn button on the NetScout Manager Plus main window (the FrameRelay and Admin radio buttons still selected).

▶ Procedure

1. Open a terminal window and go to **$NSHOME/usr**.

2. Copy an example or interface-specific file to a new file that contains the user history table number.

3. Open the new file using a text editor.

   The variables in the file are listed with their OIDs (Object IDs). The frame relay interface number 101015001 must replace @IFN, and the DLCI number to be monitored must replace @DLCI.

   Example: frCircuitSentFrames
   Change "**`1.3.6.1.2.1.10.32.2.1.6.@IFN.@DLCI`**"
   to "**`1.3.6.1.2.1.10.32.2.1.6.101015001.301`**"

   The only valid interface number for a FrameSaver SLV 9126, 9126-II, 9126-II Router, or 9128-II is 101015001.

4. Edit the new file, as needed.

Refer to *Creating .UDH Files* and *Using Custom History* in the *NetScout Manager Plus User Guide* for additional information.

See Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*, for OID information for an interface.

Installing the User-Defined History Files

Once the user-defined history files have been created, the files need to be installed. History files are installed from the command-line prompt in NetScout Manager Plus. Should the FrameSaver unit be reset, these files will need to be reinstalled. The command used to install a new user history table is located in $NSHOME/bin.

CAUTION:

Do not use user_history_table_1 or 2. UserHistory1 and UserHistory2 are the default user history files used to keep SLV data for reports. Editing either of these files will destroy SLV reporting capability.

▶ Procedure

1. Type **dvuhist -f** *agentname user_history_table_number* **config** *number_of_buckets interval download_file***.udh** to load user-defined history files for the frame relay link.

   Example:
   ```
   dvuhist -f Dallas51 3 config 30 60 Dallas51k.udh
   ```

   The interval must be entered in seconds.

2. Type **dvuhist -f “***agentname DLCI_number***”** *user_history_table_number* **config** *number_of_buckets interval download_file***.udh** to load user-defined history files for a specific DLCI.

   Example:
   ```
   dvuhist -f “Dallas51 301” 3 config 30 60 Dallas301.udh
   ```

   The same user history table number can be used for both the link and DLCI. For these examples, user history table number 3 will appear as UserHistory3 on the History List.

See Step 5 on page 10-17 in *Monitoring a DLCI’s History Data* to verify that the user-defined history files have been loaded.

Refer to *Installing .UDH Files* in *Using Custom History* of the *NetScout Manager Plus User Guide* for additional information.

Monitoring a DLCI’s History Data

Once the monitoring variables have been defined, a problem DLCI can monitored.

▶ Procedure

To monitor user history data:

1. From the NetScout Manager Plus main window, with the FrameRelay radio button still selected, select the Traffic radio button.

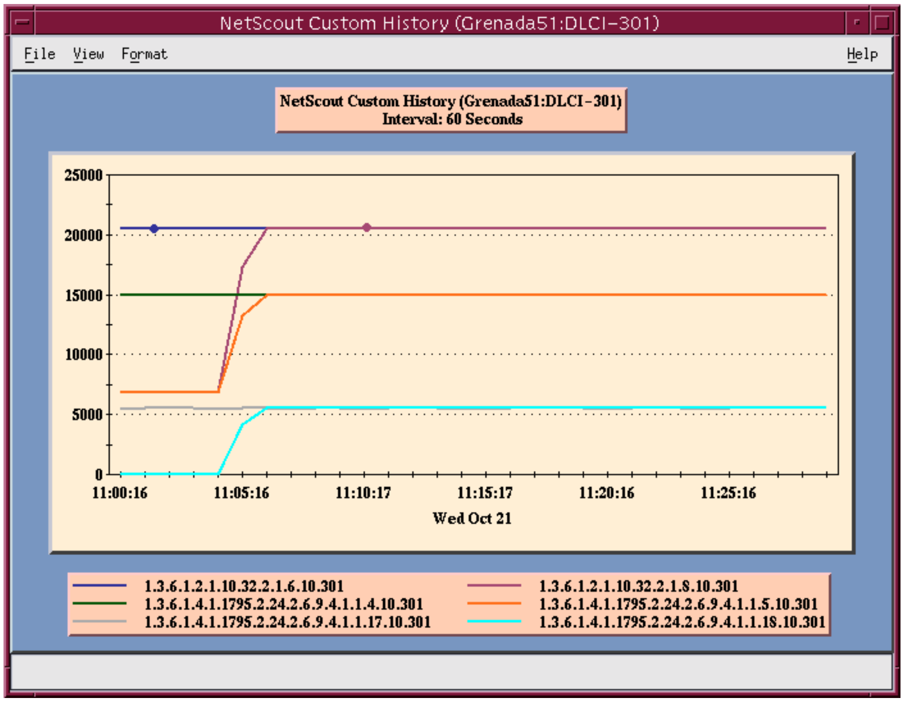
   The appropriate icons appear.

2. Highlight an agent in the agent list box so that its DLCIs appear in the DLCI list box (under the agent list box).

3. Highlight the DLCI to be monitored.

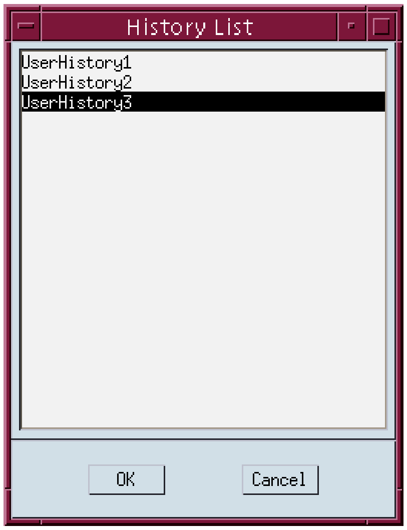
4. Click on the Custom History icon. The NetScout Custom History window opens.

   Adjust the size of the window so the entire report can be viewed.



5. Select History List from the View menu. The History List window opens.

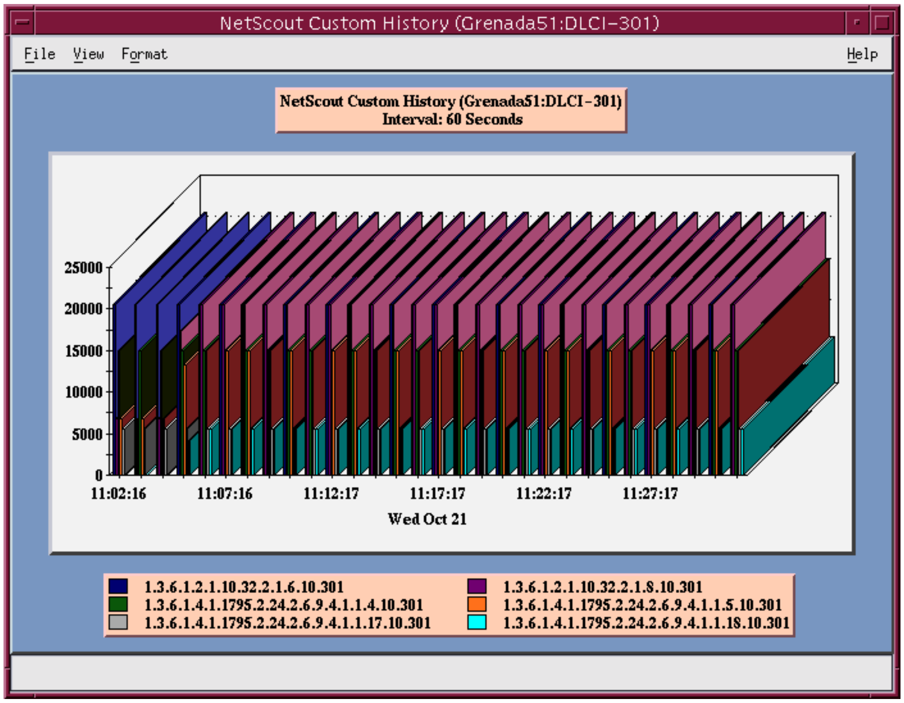
   The newly defined user history variables should appear on this list.



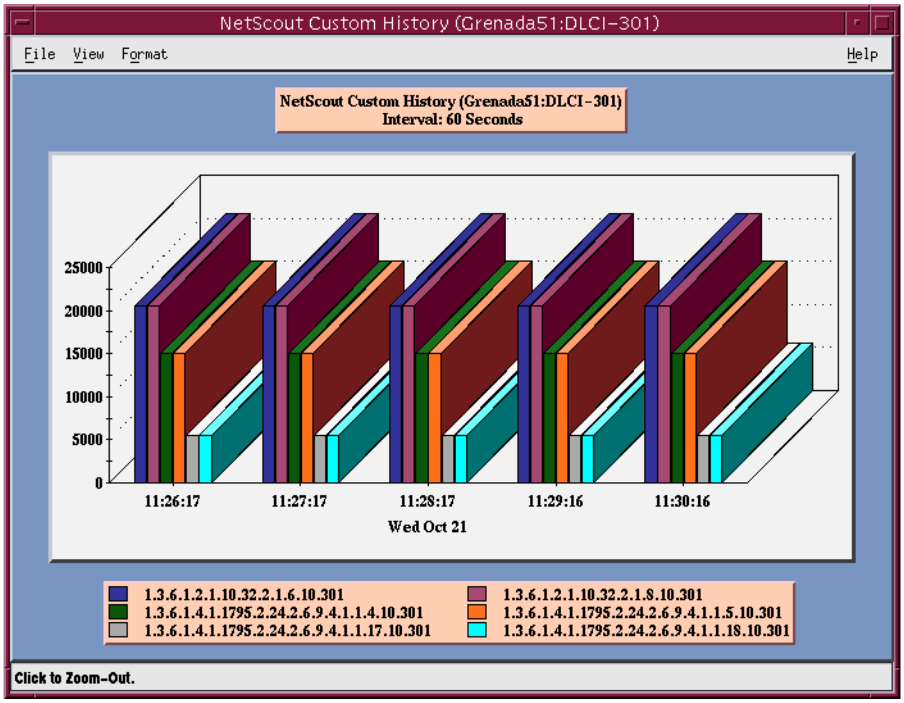
6. Highlight the desired set of user history variables, and select the OK button.

   Data is gathered based upon the configured user history variables. This may take some time, so please be patient.

7. Select 2D or 3D Bar from the Format menu, if desired (3D Bar is shown).



Using the 2D or 3D Bar to view the user history data collected, you can click on a particular bar and get an expanded view of the data.



8. Click anywhere on this window to return to the previous window view (see Step 7 on page 10-17).

Refer to *Launching User History* and *Understanding Custom History Display* in *Using Custom History* of the *NetScout Manager Plus User Guide* for additional information.

See *Object ID Cross-References (Numeric Order)* and *RMON Alarm and Event Defaults* in Appendix B, *SNMP MIBs and Traps, and RMON Alarm Defaults*, to identify OID information being shown.

Monitoring the Agent Using NetScout Manager Plus

Once the FrameSaver SLV agent has been added to NetScout Manager Plus, select either the Traffic or Protocol radio button to monitor the newly added agent, or one of its DLCIs.

NOTE:

Only the Traffic and Protocol radio buttons on the application selection bar are supported for FrameSaver SLV agents.

The procedure below describes how to monitor an agent's traffic. The procedure is the same for protocol monitoring, but you may be prompted to select a Domain Group as well as an agent or DLCI.

▶ Procedure

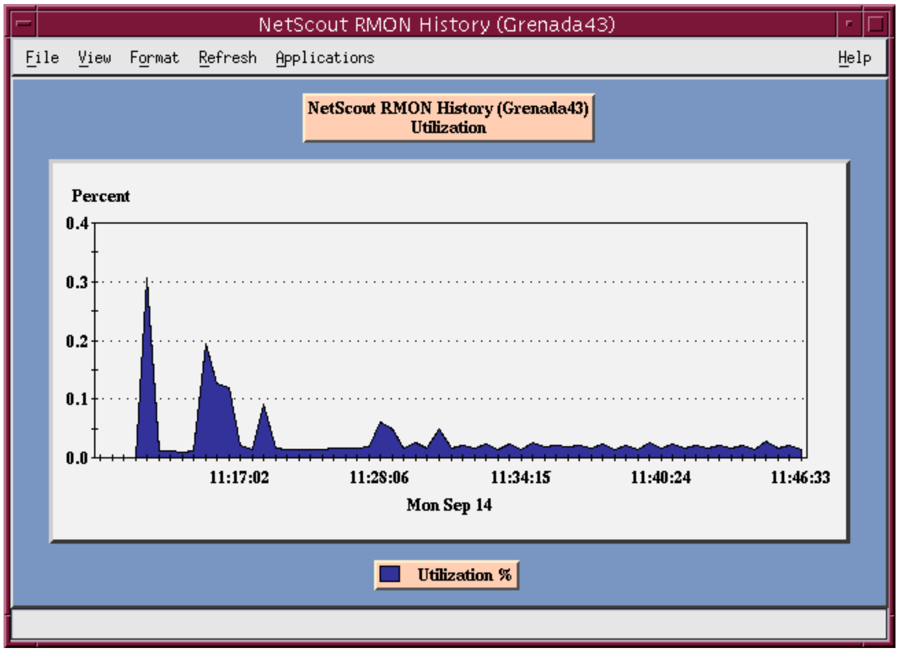
1. Select the Traffic radio button to monitor the newly added agent, or one of its DLCIs.

2. Highlight an agent in the agent list box so that its DLCIs appear in the DLCI list box (under the agent list box).

3. If you want to monitor one of the agent's DLCIs, highlight the DLCI to be monitored.

4. Click on an applicable icon. The selected graphical report should open.

   Traffic icons that would be of particular interest are Traffic Monitor and Domain History. In the example below, the Domain History icon was selected, which is actually a real-time report.



NOTE:

If Size Distribution is the selected View and distribution size has been changed via OpenLane, the values shown for the distribution will not be accurate. Only default size distributions are tracked.

Statistical Windows Supported

Not all icons that appear on the NetScout Manager Plus main window are supported for FrameSaver units. For example, All Convs (conversations) and TopNConv icons appear when the Protocol radio button is selected, but conversations are not supported.

Of the icons that appear on the NetScout Manager Plus main window, the following are supported:

Traffic Statistics	Protocol Statistics
Traffic Monitor	Protocol Monitor
Segment Zoom	Protocol Zoom
Segment Details*	TopNTalkers
Domain History*	All Talkers

* Size distribution statistics are provided for a DLCI only, not a link. If a link is selected, all size distribution statistics on the table or graph will be zero.

When a DLCI is selected, the first and last size distribution statistics are ignored for FrameSaver units and the statistics for those buckets appear in the next valid bucket (i.e., bucket size <64 and 64 statistics appear in the 65..127 bucket, and >1518 statistics appear in the 1024..1518 bucket).

Conversations and Long-Term and Short-Term Histories are not supported in this release. As a result, no data will appear on windows that include these panes.

Setting Up Network Health for FrameSaver Devices

11

FrameSaver units are compatible with Concord Communication's Network Health software. In addition, Network Health has released the first in a series of software modules that integrate FrameSaver SLV enhanced performance statistics into its reporting package (see the example in *FrameSaver SLV Plus At-a-Glance Report* on page 11-9). To get this report, you need Network Health R4.01 or higher.

This chapter includes Network Health information as it relates to FrameSaver SLV devices. It includes the following:

For additional information about installing, accessing, and managing FrameSaver SLV devices through Concord's Network Health, and for information about applicable reports, refer to:

- *Network Health Installation Guide* to help you install the application.
- *Network Health User Guide* to help you get started using the application.
- *Network Health Reports Guide* to help you understand and use Frame Relay reports.
- *Network Health – Traffic Accountant Reports Guide* to help you understand and use Traffic Accountant reports.

Installation and Setup of Network Health

Refer to the *Network Health Installation Guide* for installation instructions, and follow the instructions applicable to your network platform. Once Network Health is installed, you need to set up the application so it will support FrameSaver units.

Each Network Health application provides a different set of functions, called a module. Each module used requires a separate license to gain access to those features and functions. Make sure you license the Poller application so you can poll SLV units and collect data.

To use this application:

1. Discover network elements, units, and interfaces in the network.
2. Configure the Network Health applications, then save them.
3. Organize elements into groups for reporting purposes.
4. Set up and run reports.

Setup and operation information is contained in the *Network Health User Guide*. The sections that follow address only the minimal procedural steps needed once you have access to the applications.

See the Network Health User and Reports Guides for additional startup information and a full discussion of the application's features and how to use them.

Discovering FrameSaver Elements

Once licenses are entered and you have access to the applications, the Discover dialog box opens. Use this dialog box to search for SLV units in your network and discover their DLCIs. Saving the results of the search creates definitions in the Poller Configuration, which are used to poll the units.

IP addresses and the Community String for the FrameSaver units must be entered for Network Health to find the SLV units on the network and discover their elements. These *elements* are resources that can be polled (e.g., LAN/WAN interfaces, frame relay circuits, routers, and servers).

The two types of elements that can be polled are:

- **Statistics elements** – Provide counters and other gauges for information gathered about your network for statistical and trend analysis.
- **Conversation elements** – Provide RMON2 and similar data for information gathered about network traffic between nodes.

▶ Procedure

To find SLV device elements in your network:

1. Select the LAN/WAN radio button to specify the element type to be found. Network Health treats frame relay element discovery as a WAN element type.
2. Enter the IP Addresses of the SLV units to be located, and the Community String (Community Name in the FrameSaver unit). The Community String is case-sensitive.
3. Select the Discover button.

   The Discover dialog box closes and the Discovering dialog box opens, showing the results of the discovery process.

   A message indicates the number of elements discovered and the number of existing elements updated when the discovery process is complete. Depending upon the number of units entered and the size of your network, it could take anywhere from a few minutes to an hour or longer to discover all elements in the network.

See *Discovering Elements* in the *Network Health User Guide* for additional information and to learn how to schedule automatic element discovery updates to the database.

Configuring the Discovered Elements

Network Health sets the speed for discovered elements when it polls the unit for the first time. For a FrameSaver SLV unit, the speed set would be the unit's CIR. No additional configuration should be required. However, you should verify that all appropriate information has been retrieved.

NOTE:

If an SLV unit does not have CIR configured, or if it is not configured correctly, Network Health sets the unit's CIR to 0 Kbps. For this reason, you should reconfigure the unit's CIR before Network Health polls it. If 0 Kbps is the speed setting, you will need to edit the unit's CIR from Network Health.

Additional information can be edited, as well. See *Discovering Elements* in the *Network Health User Guide* for additional information.

▶ Procedure

To change the CIR for FrameSaver SLV unit elements from Network Health:

1. Select the Edit Before Saving button at the bottom of the Discovering dialog box once the discovery process is completed.

   The Poller Configuration window opens.

2. Double-click on the first element discovered. The Modify Element dialog box opens.

3. In the Speed box, select the Override radio button and enter the CIR for the unit in the text box.

   Letters **k** and **m** can be used as shortcuts (e.g., enter 56 k for 56 kilobits per second, or 16 m for 16 Mbits per second).

4. Apply your changes:

   — Select the Apply/Next button to save your change and bring up the next element to be edited. Continue until all newly discovered frame relay elements have been modified before selecting the OK button.

   — Select the the OK button.

   The Modify Element dialog box closes.

5. Select the OK button at the bottom of the Poller Configuration window. The modified elements are saved to the database, and the units are polled.

Allow Network Health to continue polling for about a half an hour to allow time for data to be gathered before running any reports.

Grouping Elements for Reports

Once the discovery process is completed and required changes are made, the newly discovered elements (DLCIs) should be organized into a group for Health reporting. Grouping makes for easier monitoring and management of similar node types (e.g., all SLV elements). Once grouped, you can then run reports on all DLCIs in the network, as well as reports on individual DLCIs.

▶ Procedure

To group elements:

1. From the console, select Edit Groups from the Reports menu. The Add Groups dialog box opens.
2. Enter a name in the Group Name field. Up to 64 characters can be entered. A through Z, a through z, 0 through 9, dashes (–), periods (.), and underscores (_) can be used. No spaces can be included, and the word All cannot be used.
3. Select the WAN radio button (above the Available Elements list).
4. Highlight all the DLCIs listed on the Available Elements list, or select specific DLCIs, then select the left arrow button.

   The highlighted DLCIs move from the Available Elements list to the Group Members list.
5. Select the OK button when all appropriate DLCIs have been moved to the Group Members list.

   The Add Groups dialog box closes and the newly created group appears on the Groups dialog box.

See *Managing Groups and Group Lists* in the *Network Health Reports Guide* for additional information. That chapter also tells you how to customize reports.

Generating Reports for a Group

Once Network Health has had sufficient time to gather data from the polled DLCIs and the DLCIs have been grouped, you can start generating reports. When selecting a report Section, select WAN from the drop-down list. See *Running Reports from the Console* in the *Network Health Reports Guide* for additional information. That section also tells you how to schedule automatic report generation.

NOTE:

Network Health provides information with each chart or table, generally referred to as a report. Click on the hyperlink (Explanation of...) for an explanation of the report and its features. You can also refer to the *Network Health Reports Guide*.

About Service Level Reports

For long-term analysis and reporting, you will want to license the Service Level Reports application. This application analyzes data collected over months, or by quarters, and provides service level information about an enterprise, a region, department, or business process. Executive, IT Manager, and Customer Service Level reports are provided.

Using these reports, you can measure service performance against goals and agreements. Ranges for service level goals can be set for up to five variables: availability, bandwidth, bytes, health exceptions, and latency. These ranges need to be set before reports are scheduled.

About At-a-Glance Reports

At-a-Glance Reports consolidate various important DLCI and network performance indicators onto a single page. Up to ten DLCIs can be included in an At-a-Glance Report.

Using the *FrameSaver SLV Plus At-a-Glance Report* on page 11-9, you can compare a DLCI’s volume with the network’s performance over a specified period of time. Ranges for service level goals can be set for up to five variables: availability, bandwidth, bytes, health exceptions, and latency. These ranges need to be set before reports are scheduled. In addition, all the enhanced network statistics that only an SLV device can accurately collect is provided so you can truly monitor the health of the frame relay network and see the effects of the customer’s utilization on network efficiency.

About Trend Reports

By specifying specific variables like bandwidth, trend analysis can be performed and shown on Trend Reports. Up to ten variables for a DLCI, or ten DLCIs on one variable can be generated on a single trend report. Information can be presented in a line graph, pie chart, bar chart, or table format. Any amount of time can be specified for the reporting period.

These reports can help identify the reasons a DLCI has acquired a poor Health Index rating. See the Exceptions Report for information about Health Index ratings.

Printed Reports

All of the charts and tables seen online can also be provided on printed reports.

Reports Applicable to SLV Devices

The following frame relay reports support FrameSaver SLV units:

- **Exception Reports** – Provide summary and detail information that identifies DLCIs with the highest incidence of errors, high bandwidth utilization, and trends.

  These reports identify those DLCIs that have exceeded a specified number of accumulated *exception points*. It is a good idea to run this report daily so that DLCIs having the most problems can be attended to first. DLCIs contained on this report need immediate attention.

  If a DLCI suddenly shows up on these reports, check whether any new equipment has been added to the network and whether it is properly configured. If its configuration is correct, the equipment could be faulty.

- **Summary Reports** – Provide summary information for the network, volume and error leaders, and DLCI traffic.

  — **Network Summary Report** – Provides an overall view of the network. Use this report for planning and to predict when a DLCI might run into problems.

  — **Leaders Summary Report** – Identifies DLCIs having the highest volume and errors. High traffic volume may be increasing latency, and the high Health Index rating indicates problems. It is a good idea to run these reports daily so a norm can be established. The same DLCIs should appear.

  Use this chart and table to alert you to possible problems. Problems to look for include: a normally high-volume DLCI is dropped from the list, a new DLCI appears on the list (check Element Summaries), a DLCI has a high Health Index rating, but low volume, significant differences between a DLCI’s average and peak Health Index rating.

  - **Elements Summary Report** – Compares DLCI traffic with volume and the baseline, bandwidth utilization, and errors.

    Use this report for DLCI detail information and comparison, to identify DLCIs with above or below average volume so they can be investigated when there are any significant changes.

- **Supplemental Report** – Shows DLCI availability and latency. The information shown in this report is also on other Health reports. However, these charts show more than ten DLCIs at a time so you have a broader view of the service provided by the network.

- **Service Level Reports** – Provide summary information for a group list for a longer reporting period than other reports.

  - **Executive Service Level Report** – Provides service level performance for an enterprise on a single page. Use this report to assess whether IT service levels are meeting availability and service goals.

  - **IT Manager Service Level Report** – Provides service level information for various groups. Using this report, you can compare service level performance of various groups. The report summarizes service levels for a group of DLCIs, along with details on individual DLCIs within that group.

  - **Customer Service Level Report** – Provides service level information for customers. This report is used to provide service level information to service customers to help them determine optimum service levels needed based upon their own traffic data, as well as provide documented evidence for increasing CIR. It combines daily volume, daily Health exceptions, bandwidth distribution, average Health Index ratings and availability for each DLCI onto a single page.

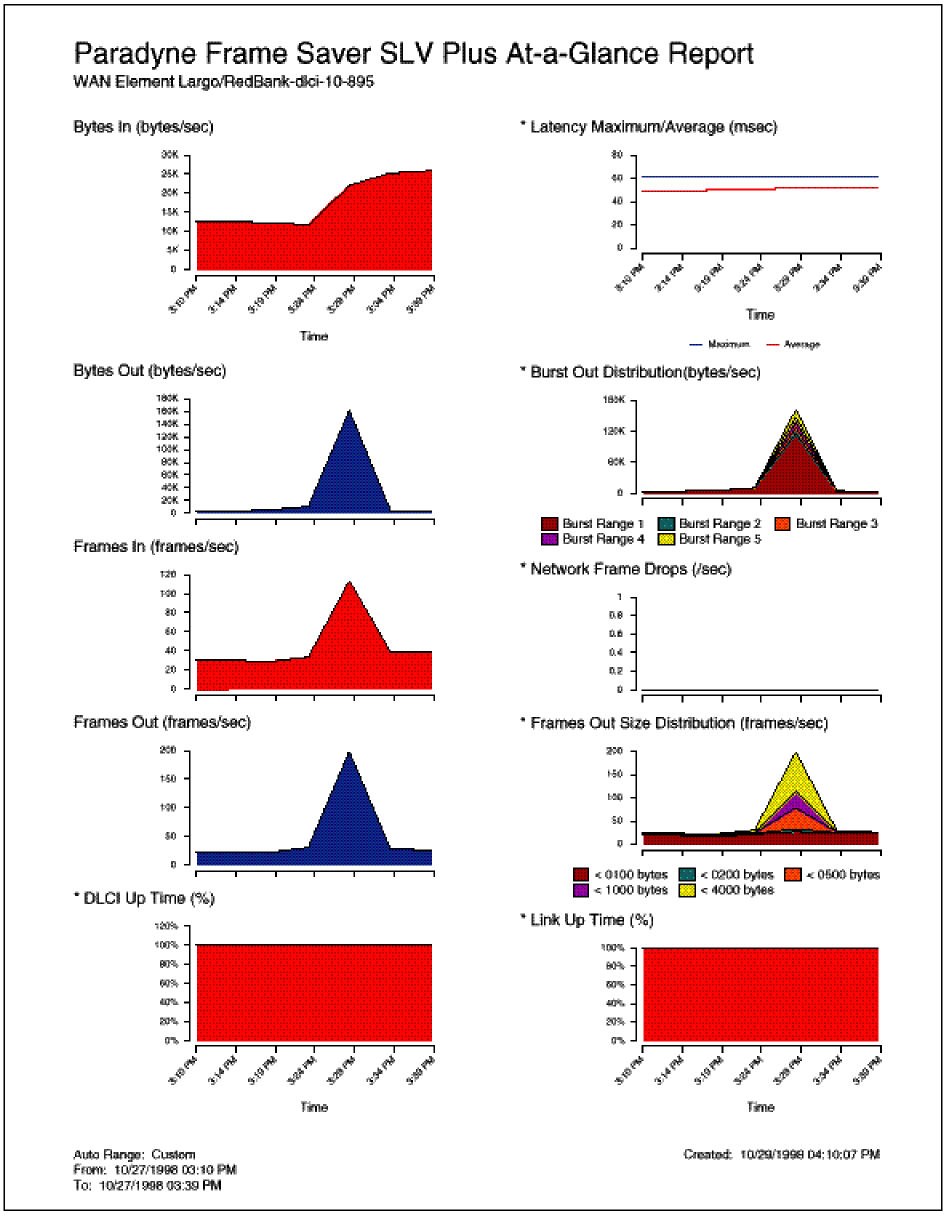
- **At-a-Glance Reports** – Provides consolidated DLCI and network performance information onto a single page.

  - **At-a-Glance Report** – Consolidates bandwidth utilization, network traffic, events occurring over the reporting period, and availability and latency levels information. Variables other than bandwidth can be selected for a trend report (e.g., burst octets), but a bandwidth trend report should be generated when investigating problems that appear on Exceptions Reports, Supplemental Reports, and Health reports.

    Use trend reports to view individual variables for DLCIs having a high Health Index rating to help locate which variable is causing a problem leading to a DLCI’s poor Health Index rating.

— **FrameSaver SLV Plus At-a-Glance Report**

Performs trend analysis on up to ten specified variables for DLCIs. This is the first Network Health report to integrate the FrameSaver SLV's unique monitoring capabilities, using the unit's SLV-enhanced network statistics.



Paradyne Frame Saver SLV Plus At-a-Glance Report

WAN Element Largo/RedBank-dlci-10-895

Bytes In (bytes/sec)

* Latency Maximum/Average (msec)

Bytes Out (bytes/sec)

* Burst Out Distribution(bytes/sec)

Burst Range 1 · Burst Range 2 · Burst Range 3 · Burst Range 4 · Burst Range 5

Frames In (frames/sec)

* Network Frame Drops (/sec)

Frames Out (frames/sec)

* Frames Out Size Distribution (frames/sec)

< 0100 bytes · < 0200 bytes · < 0500 bytes · < 1000 bytes · < 4000 bytes

* DLCI Up Time (%)

* Link Up Time (%)

Auto Range: Custom
From: 10/27/1998 03:10 PM
To: 10/27/1998 03:39 PM

Created: 10/29/1998 04:10:07 PM

- **Trend Reports** – Perform trend analysis on up to ten specified variables for DLCIs. Variables other than bandwidth can be selected for a trend report (e.g., burst octets), but a bandwidth trend report should be generated when investigating problems that appear on Exceptions Reports, Supplemental Reports, and Health reports.

  Use trend reports to view individual variables for DLCIs having a high Health Index rating to help locate which variable is causing a problem leading to a DLCI’s poor Health Index rating.

See the *Network Health Reports Guide* for more information about these reports.

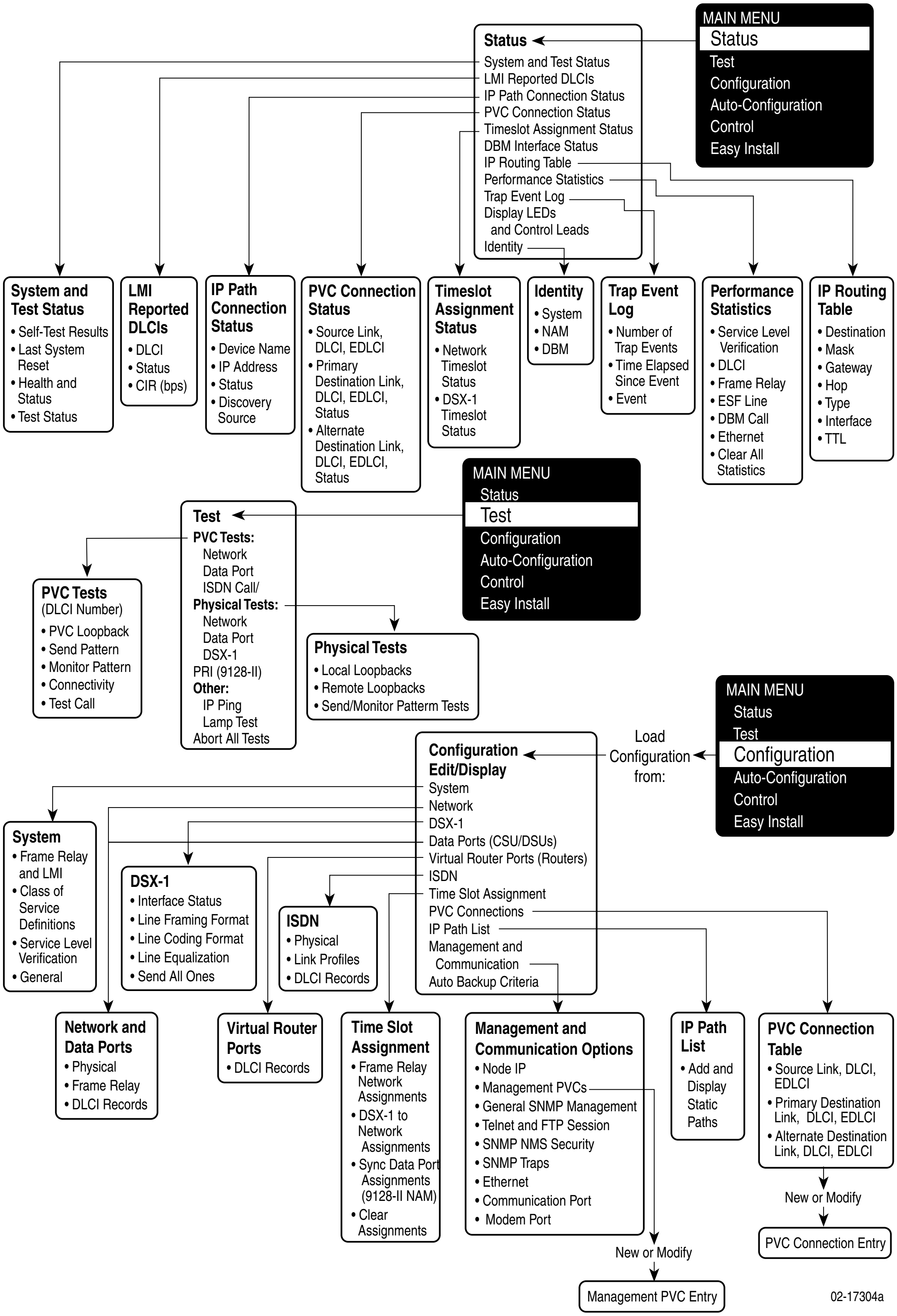
Menu Hierarchy

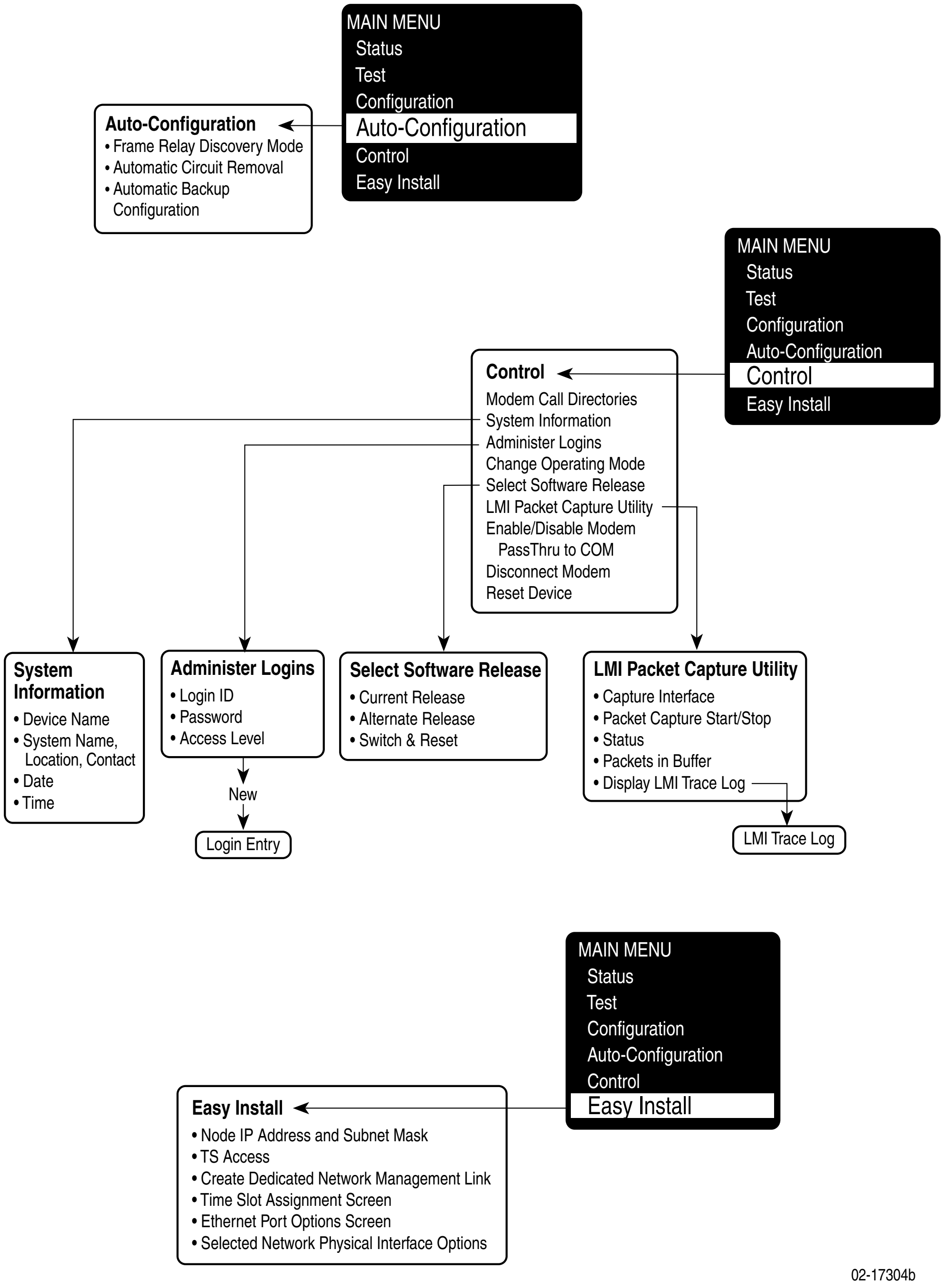
A

Menus

The Menu Hierarchy on the following pages shows a pictorial view of the organization of the FrameSaver CSU/DSU and Router's screens, which can help you navigate the menus and access information.

ISDN backup and Data Ports options do not apply to the router. The Virtual Router Ports option does not apply to the CSU/DSUs.


MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Easy Install
Status
System and Test Status
LMI Reported DLCIs
IP Path Connection Status
PVC Connection Status
Timeslot Assignment Status
DBM Interface Status
IP Routing Table
Performance Statistics
Trap Event Log
Display LEDs and Control Leads
Identity
System and Test Status
• Self-Test Results
• Last System Reset
• Health and Status
• Test Status
LMI Reported DLCIs
• DLCI
• Status
• CIR (bps)
IP Path Connection Status
• Device Name
• IP Address
• Status
• Discovery Source
PVC Connection Status
• Source Link, DLCI, EDLCI
• Primary Destination Link, DLCI, EDLCI, Status
• Alternate Destination Link, DLCI, EDLCI, Status
Timeslot Assignment Status
• Network Timeslot Status
• DSX-1 Timeslot Status
Identity
• System
• NAM
• DBM
Trap Event Log
• Number of Trap Events
• Time Elapsed Since Event
• Event
Performance Statistics
• Service Level Verification
• DLCI
• Frame Relay
• ESF Line
• DBM Call
• Ethernet
• Clear All Statistics
IP Routing Table
• Destination
• Mask
• Gateway
• Hop
• Type
• Interface
• TTL
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Easy Install
Test
PVC Tests:
Network
Data Port
ISDN Call/
Physical Tests:
Network
Data Port
DSX-1
PRI (9128-II)
Other:
IP Ping
Lamp Test
Abort All Tests
PVC Tests
(DLCI Number)
• PVC Loopback
• Send Pattern
• Monitor Pattern
• Connectivity
• Test Call
Physical Tests
• Local Loopbacks
• Remote Loopbacks
• Send/Monitor Patterm Tests
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Easy Install
Load Configuration from:
Configuration Edit/Display
System
Network
DSX-1
Data Ports (CSU/DSUs)
Virtual Router Ports (Routers)
ISDN
Time Slot Assignment
PVC Connections
IP Path List
Management and Communication
Auto Backup Criteria
System
• Frame Relay and LMI
• Class of Service Definitions
• Service Level Verification
• General
DSX-1
• Interface Status
• Line Framing Format
• Line Coding Format
• Line Equalization
• Send All Ones
ISDN
• Physical
• Link Profiles
• DLCI Records
Network and Data Ports
• Physical
• Frame Relay
• DLCI Records
Virtual Router Ports
• DLCI Records
Time Slot Assignment
• Frame Relay Network Assignments
• DSX-1 to Network Assignments
• Sync Data Port Assignments (9128-II NAM)
• Clear Assignments
Management and Communication Options
• Node IP
• Management PVCs
• General SNMP Management
• Telnet and FTP Session
• SNMP NMS Security
• SNMP Traps
• Ethernet
• Communication Port
• Modem Port
New or Modify
Management PVC Entry
IP Path List
• Add and Display Static Paths
PVC Connection Table
• Source Link, DLCI, EDLCI
• Primary Destination Link, DLCI, EDLCI
• Alternate Destination Link, DLCI, EDLCI
New or Modify
PVC Connection Entry
02-17304a


MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Easy Install
Auto-Configuration
• Frame Relay Discovery Mode
• Automatic Circuit Removal
• Automatic Backup Configuration
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Easy Install
Control
Modem Call Directories
System Information
Administer Logins
Change Operating Mode
Select Software Release
LMI Packet Capture Utility
Enable/Disable Modem PassThru to COM
Disconnect Modem
Reset Device
System Information
• Device Name
• System Name, Location, Contact
• Date
• Time
Administer Logins
• Login ID
• Password
• Access Level
New
Login Entry
Select Software Release
• Current Release
• Alternate Release
• Switch & Reset
LMI Packet Capture Utility
• Capture Interface
• Packet Capture Start/Stop
• Status
• Packets in Buffer
• Display LMI Trace Log
LMI Trace Log
MAIN MENU
Status
Test
Configuration
Auto-Configuration
Control
Easy Install
Easy Install
• Node IP Address and Subnet Mask
• TS Access
• Create Dedicated Network Management Link
• Time Slot Assignment Screen
• Ethernet Port Options Screen
• Selected Network Physical Interface Options
02-17304b

SNMP MIBs and Traps, and RMON Alarm Defaults

B

This appendix contains the following:

MIB Support

The FrameSaver unit supports the SNMP Version 1, and has the capability of being managed by any industry-standard SNMP manager and accessed by external SNMP managers using SNMP protocol.

The following MIBs are supported:

- MIB II (RFC 1213 and RFC 1573)
- Frame Relay DTEs MIB (RFC 2115)
- DS1/E1 MIB (RFC 1406)
- RS-232-Like MIB (RFC 1659)
- Frame Relay Service MIB (RFC 1604)
- Enterprise MIB
- Dial Control MIB using SMIv2 (RFC 2128)
- RMON Version 1 MIB (RFC 1757)
- RMON Version 2 MIB (RFC 2021)

Downloading MIBs and SNMP Traps

Paradyne standard and enterprise MIBs are available from the Paradyne World Wide Web site.

▶ Procedure

To access Paradyne MIBs:

1. Access the Paradyne World Wide Web site at **www.paradyne.com**.
2. Select Technical Support.
3. Select Management Information Base (MIBs).

The download procedure may vary depending upon your browser or NMS application software. Refer to your browser or NMS manual for additional download information.

System Group (mib-2)

This section provides the system object identifier and system description for the System Group for the FrameSaver unit, which is an SNMPv1 MIB.

FrameSaver Unit's sysDescr (system 1)

The following is the system description (sysDescr [system 1]) for the NMS subsystem in the FrameSaver unit:

> PARADYNE T1 FrameSaver SLV; Model: *[9126/9126-II/9126-IIR/9128-II]*; S/W Release: *(MM.mm.bb [Major.minor.build] format)*; NAM CCA number: *(hardware version in hhhh-hhh format)*; Serial number: *sssssss*

FrameSaver Unit's sysObjectID (system 2)

The following is the system object identifier (sysObjectID [system 2]), or OID, for the NMS subsystem in the FrameSaver units:

FrameSaver SLV 9126-SLV:	1.3.6.1.4.1.1795.1.14.2.4.4.7
FrameSaver SLV 9126-II:	1.3.6.1.4.1.1795.1.14.2.4.4.7.1
FrameSaver SLV 9126-IISLV:	1.3.6.1.4.1.1795.1.14.2.4.4.7
FrameSaver SLV 9126-IIR:	1.3.6.1.4.1.1795.1.14.2.4.11.4.1
FrameSaver SLV 9126-IIRSLV:	1.3.6.1.4.1.1795.1.14.2.4.11.4
FrameSaver SLV 9128-II:	1.3.6.1.4.1.1795.1.14.2.4.4.8.1
FrameSaver SLV 9128-IISLV:	1.3.6.1.4.1.1795.1.14.2.4.4.8

Interfaces Group (mib-2)

Clarification for objects in the Interfaces Group, as defined in RFC 1573 and RFC 1213, which is an SNMPv1 MIB, is provided in this section.

Paradyne Indexes to the Interface Table (ifTable)

The following table provides the ifName for each interface type, the ifDescr, and the ifIndex that Paradyne has assigned to each.

Table B-1. Paradyne Interface Objects Information (1 of 3)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Physical Layer			
Network T1	T1 network interface	Network T1; T1 FR NAM; Hardware Version: *hhhh-hhh*	101001001
DSX-1 T1	DSX-1 interface	DSX-1 T1; T1 FR NAM; Hardware Version: *hhhh-hhh*	101002001
Sync Data Port S01P1	Synchronous Data Port-1	Synchronous Data Port, Slot: 1, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	101003001

Table B-1. Paradyne Interface Objects Information (2 of 3)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Physical Layer *(continued)*			
Sync Data Port S01P2	Synchronous Data Port-2 (if applicable)	Synchronous Data Port, Slot: 1, Port: 2; T1 FR NAM; Hardware Version: *hhhh-hhh*	101003002
COM	Communications port	COM Port; T1 FR NAM; Hardware Version: *hhhh-hhh*	101004001
Modem	Modem port	Modem Port; T1 FR NAM; Hardware Version: *hhhh-hhh*	101005001
ISDN BRI DBM	ISDN BRI DBM interface (if applicable)	ISDN BRI DBM; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101110001
ISDN PRI DBM	ISDN PRI DBM interface (if applicable)	ISDN PRI DBM; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101111001
Frame Relay Logical Layer			
FR Bundle	Multilink Frame Relay (MFR) Bundle	FR Bundle, Profile: *[Link Name]*; Hardware Version: *hhhh-hhh*	*9126:* 101025001 to 101025051 *9128:* 101025001 to 101025120
FR UNI	Frame relay logical link on the T1 network interface	*For the DTE side:* Network T1 of FR DTE; T1 FR NAM; Hardware Version: *hhhh-hhh*	101015001
		For the DCE side: Network T1 of FR SERVICE; T1 FR NAM; Hardware Version: *hhhh-hhh*	
	Frame relay logical link on the Sync Data Port-1	*For the user side:* Synchronous Data Port of FR DTE, Slot: *s*, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	101016001
		For the network side: Synchronous Data Port of FR SERVICE, Slot: *s*, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	

Table B-1. Paradyne Interface Objects Information (3 of 3)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer *(continued)*			

FR UNI	Frame relay logical link on the Sync Data Port-2 (if applicable)	*For the user side:*
		Synchronous Data Port of FR DTE, Slot: *s*, Port: 2;
		T1 FR NAM;
		Hardware Version: *hhhh-hhh*
			101016002

		For the network side:
		Synchronous Data Port of FR SERVICE, Slot: *s*, Port: 2;
		T1 FR NAM;
		Hardware Version: *hhhh-hhh*	

	Frame relay logical link on BRI (if applicable)	*For the user side:*
		ISDN BRI DBM of FR DTE;
		Profile: *[Link Name]*; T1 FR NAM;
		Child Card: ISDN-BRI DBM;
		S/W Release: *MM.mm.bb*;
		Hardware Version: *hhhh-hhh*
			101018001
			101018002

		For the network side: ISDN BRI DBM of FR SERVICE; Profile: *[Link Name]*; T1 FR NAM; Child Card: ISDN-BRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101018001 101018002
	Frame relay logical link on PRI (if applicable)	*For the user side:* ISDN PRI DBM of FR DTE; Profile: *[Link Name]*; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	101017001 to 101017024
		For the network side: ISDN PRI DBM of FR SERVICE; Profile: *[Link Name]*; T1 FR NAM; Child Card: ISDN-PRI DBM; S/W Release: *MM.mm.bb*; Hardware Version: *hhhh-hhh*	

NetScout Indexes to the Interface Table (ifTable)

For remote monitoring at sites where FrameSaver units are operating with NetScout Probes, use the following ifName, ifDescr, and ifIndex.

Table B-2. NetScout Interface Objects Information (1 of 2)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
Frame Relay Logical Layer			
Frame Relay 1 Network	Frame relay logical link on the network interface	*For the DTE side:* RMON (IN/OUT); Network T1 of FR DTE; T1 FR NAM; Hardware Version: *hhhh-hhh*	1
		For the DCE side: RMON (IN/OUT); Network T1 of FR SERVICE; T1 FR NAM; Hardware Version: *hhhh-hhh*	
Frame Relay 3 Sync Data Port 1	Frame relay logical link on Synchronous Data Port-1	*For the user side:* RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: *s*, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	3
		For the network side: RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: *s*, Port: 1; T1 FR NAM; Hardware Version: *hhhh-hhh*	
Frame Relay 4 Sync Data Port 2	Frame relay logical link on Synchronous Data Port-2	*For the user side:* RMON (IN/OUT); Synchronous Data Port of FR DTE, Slot: *s*, Port: 2; T1 FR NAM; Hardware Version: *hhhh-hhh*	4
		For the network side: RMON (IN/OUT); Synchronous Data Port of FR SERVICE, Slot: *s*, Port: 2; T1 FR NAM; Hardware Version: *hhhh-hhh*	

Table B-2. NetScout Interface Objects Information (2 of 2)

ifName	Description	ifDescr (ifEntry 2)	ifIndex
RMON Logical Layer			
RMON Frame Relay Logical Interfaces	These values are calculated. ■ For the DTE: (ifIndex –1) * 2 +17 ■ For the DCE: DTE calculated value +1	IN – RMON (IN); [*ifName of the interface*]	17–48
		OUT – RMON (OUT); [*ifName of the interface*]	
RMON Virtual Interfaces	These values are calculated based on the probe's internal circuit index: circuit index +65.	ALL – VIRTUAL PVC [*interface number*] [*DLCI number*] ALL	65–512
RMON Virtual Logical Interfaces	These values are calculated. ■ For the DTE: (virtual interface ifIndex –65) * 2 +513 ■ For the DCE: DTE calculated value +1	IN – VIRTUAL PVC [*interface number*] [*DLCI number*] DTE	513–1023
		OUT – VIRTUAL PVC [*interface number*] [*DLCI number*] DCE	

Standards Compliance for SNMP Traps

This section describes the FrameSaver unit's compliance with SNMP format standards and with its special operational trap features.

All traps have an associated string to help you decipher the meaning of the trap. Strings associated with an interface with a substring containing $ifString have the following format:

'DLCI $dlciNumber "$circuitId" of $ifName frame relay link "$linkName".'

— $dlciNumber is the DLCI number. DLCI $dlciNumber "$circuitId" only appears when a DLCI is associated with the trap.

— $circuitId is the name given to the circuit. It can be an empty string, or a 1–64 byte string within quotes (e.g., "Chicago to New York"), and only appears when a DLCI with "circuitID" is associated with the trap.

— $linkName is the name given to the link. Frame relay $linkName only appears when a frame relay link has been named and is associated with the trap.

— $ifName is the string returned for the SNMP ifName variable.

Examples:
'DLCI 100 "Chicago to New York" of Network T1 frame relay link' In this example, a DLCI and a frame relay link are associated with the trap.

Typically, the $circuitId is a coded string encoded by the network service provider. The following shows an example.
'DLCI 100 "cc0402–dec0704.RG21" of Network T1 frame relay link'

The unit supports the following:

- *Trap: warmStart*
- *Trap: authenticationFailure*
- *Traps: linkUp and linkDown*
- *Traps: enterprise-Specific*
- *Traps: RMON-Specific*
- *Trap: dialControl*

These traps are listed in alphabetical order within each table.

Trap: warmStart

This trap indicates that the FrameSaver unit has been reset and has stabilized.

Table B-3. warmStart Trap

Trap	What It Indicates	Possible Cause
warmStart	FrameSaver unit has just reinitialized and stabilized itself.	■ Reset command sent. ■ Power disruption. *String:* ‘Unit reset.’
	Variable-Binding	
	devLastTrapString (devHealthAndStatus.mib)	

Trap: authenticationFailure

This trap indicates that access to the FrameSaver unit was unsuccessful due to lack of authentication.

Table B-4. authenticationFailure Trap

Trap	What It Indicates	Possible Cause
authenticationFailure	Access to the FrameSaver unit was attempted and failed.	■ Bad password on COM port terminal. *String:* ‘Unauthorized access attempted from COM port.’ ■ Bad password on modem port terminal. *String:* ‘Unauthorized access attempted from modem port.’ ■ Bad password through telnet. *String:* ‘Unauthorized access attempted from telnet user at $ipAddress.’ ■ SNMP bad community, unauthorized IP address, or unauthorized operation. *String:* ‘Unauthorized access attempted from SNMP user at $ipAddress.’
authenticationFailure	**Variable-Binding**	■ An ISDN backup call has been received, but the call was rejected. *String:* ‘Bad Caller ID $phone.’ ($phone is either a phone number or “no number.”)
	devLastTrapString (devHealthAndStatus.mib)	

Traps: linkUp and linkDown

These traps are supported on the following interfaces:

- Network, DSX-1, and synchronous data ports – Physical sublayer interfaces
- Frame relay logical link layer interfaces

Table B-5. linkUp and linkDown Traps

Trap	What It Indicates	Possible Cause
linkDown	A failure in one of the communication interfaces has occurred.	A failure in one of the communication interfaces has occurred.
linkUp	One of the failed communication interfaces is up and operational.	One of the failed communication interfaces is up and operational.

linkUp and linkDown variable-bindings are in Table B-6, linkUp and linkDown Variable-Bindings.

Physical and logical sublayers are represented by the entry in the MIB II Interfaces Table. It is supported by a combination of the Frame Relay Extension MIB and either the Frame Relay Services MIB or the Frame Relay DTEs MIB.

Table B-6. linkUp and linkDown Variable-Bindings (1 of 2)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer		
T1 Network, DSX-1, PRI (Supported by the media-specific DS1 MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the interface. Alarm conditions include: – Loss of Signal (LOS) or far-end loss of signal – Out of Frame (OOF) – Alarm Indication Signal (AIS) – Excessive Error Rate (EER) – Yellow Alarm *Strings:* ‘$ifString down.’ No alarms exist. (e.g., ‘Network T1 down due to yellow alarm.’) ‘$ifString administratively shutdown.’ (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. *String:* ‘$ifString up.’
Synchronous Data Port (Supported by the media-specific RS232-like MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the port. Alarm conditions include: – DTR off[1] – RTS off[2] – ‘ ’ – Not DTR or RTS, but link is down. *String:* ‘$ifString $alarmString down.’ (e.g., ‘Sync Data Port S01P1 DTR and RTS down.’) ‘$ifString administratively shutdown.’ (Due to an intentional shutdown.) ■ linkUp – No alarms on the port. *String:* ‘$ifString up.’

[1] The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state.

[2] The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state.

[3] If the LMI Protocol is not configured, a linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled.

Table B-6. linkUp and linkDown Variable-Bindings (2 of 2)

Interface	Variable-Bindings	Possible Cause
Physical Sublayer *(continued)*		
BRI (Supported through ifIndex – RFC 1573.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – One or more alarm conditions are active on the interface. *Strings:* '$ifString down.' No alarms exist on the link. '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – No alarms on the interface. *String:* '$ifString up.'
Logical Link Sublayer		
T1 Network, BRI, PRI, Synchronous Data Port Service Side of the Frame Relay UNI (Supported by the media-specific Frame Relay Services MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled. *Strings:* '$ifString down.' No alarms exist on the link due to LMI. '$ifString LMI down.' No alarms exist on the link. (e.g., 'Sync Data Port S01P1 frame relay link "Port-1" LMI down.') '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'
T1 Network, BRI, PRI, Synchronous Data Port DTE Side of the Frame Relay UNI (Supported by the media-specific Frame Relay DTE's MIB.)	■ ifIndex (RFC 1573) ■ ifAdminStatus (RFC 1573) ■ ifOperStatus (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib)	■ linkDown – LMI is down for the LMI Protocol configured,[3] or Frame Relay link is disabled. *Strings:* '$ifString LMI down.' '$ifString administratively shutdown.' (Due to an intentional shutdown.) ■ linkUp – LMI is up or Frame Relay link is enabled. *String:* '$ifString up.'

[1] The DTR alarm condition will only generate a linkUp/linkDown trap if the DTE supports the DTR lead state.

[2] The RTS alarm condition will only generate a linkUp/linkDown trap if the DTE supports the RTS lead state.

[3] If the LMI Protocol is not configured, a linkUp/linkDown trap is based solely upon whether the interface is enabled or disabled.

Traps: enterprise-Specific

These traps indicate that an enterprise-specific event has occurred. Supported enterprise-specific traps are listed below.

Table B-7. enterprise-Specific Traps and Variable-Bindings (1 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseCIR-Change(15)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciCIR (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib)	CIR has changed due to the LMI report. LMI Protocol is set to Standard and the network’s CIR changed. *String:* ‘CIR on $ifString changed to $CIR bps.’
enterpriseConfig-Change(6)	■ devLastTrapString (devHealthAndStatus.-mib)	Configuration has been changed via the menu-driven user interface, an SNMP Manager, or auto-configuration after 60 seconds has elapsed without another change. *String:* ‘Device configuration change.’
enterpriseDLCI-delete (17)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.-mib.)	The DLCI has been deleted. The network no longer supports the DLCI, and it was removed. *Strings:* ‘$ifString deleted by Auto-DLCI delete.’’
enterpriseDLCI-Down(11)		DLCI Status is set to Inactive; the DLCI is down. *Strings:* ‘$ifString down.’ (Due to LMI or physical failure.) ‘$ifString administratively shutdown.’ (Due to an intentional shutdown.)
enterpriseDLCIUp(12)		DLCI Status is set to Active; DLCI is up again. *String:* ‘$ifString up.’
enterpriseLatency-Exceeded(21)	■ ifIndex (RFC 1573) ■ devLastTrapString (devHealthAndStatus.-mib	An IP SLV latency threshold has been exceeded for a particular Class of Service for a path. *String:* ‘Latency exceeded *xxx.xxx.xxx.xxx*, COS *nn*, DLCI *nnnn*’

Table B-7. enterprise-Specific Traps and Variable-Bindings (2 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseMissedSLVDown(16)	■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devFrExtDlciMissedSLVs (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.mib.)	Received SLV communications have been missed; SLV Timeout Error Event Threshold has been exceeded. *String:* 'SLV down on $ifString due to excessive SLV packet loss. Total SLV packets lost is $numLost.'
enterpriseMissedSLVUp(116)		SLV Timeout Error Event has been cleared. *String:* 'SLV up on $ifString because SLV communication was reestablished. Total SLV packets lost is $numLost.'
enterprisePathDown(19)	■ ifIndex (RFC 1573) ■ devLastTrapString (devHealthAndStatus.mib	A path on the network interface has become unavailable. *String:* 'Path *xxx.xxx.xxx.xxx* Down, DLCI *nnnn*'
enterprisePathUp(20)	■ ifIndex (RFC 1573) ■ devLastTrapString (devHealthAndStatus.mib	A path on the network interface has become available. *String:* 'Path *xxx.xxx.xxx.xxx* Up, DLCI *nnnn*'
enterprisePrimaryClockFail(1)	■ devLastTrapString (devHealthAndStatus.mib)	Operating software has detected that the primary clock source has failed. *String:* 'Primary clock failed.'
enterprisePrimaryClockFailClear(101)		Operating software has detected that the primary clock source is operational again. *String:* 'Primary clock restored.'
enterpriseRMONResetToDefault(13)	■ devLastTrapString (devHealthAndStatus.mib)	All RMON-related option changes have been reset to their default values. Default Factory Configuration settings have been reloaded, returning RMON-related options to their original settings. *String:* 'RMON database reset to defaults.'

Table B-7. enterprise-Specific Traps and Variable-Bindings (3 of 3)

Trap	Variable-Bindings	Possible Cause
enterpriseSecondaryClockFail(4)	■ devLastTrapString (devHealthAndStatus.mib)	Operating software has detected that the secondary clock source has failed. *String:* ‘Secondary clock failed.’
enterpriseSecondaryClockFailClear(104)		Operating software has detected that the secondary clock source is operational again. *String:* ‘Secondary clock restored.’
enterpriseSelfTestFail(2)	■ devLastTrapString (devHealthAndStatus.mib)	Unit has completed (re)initialization and a hardware failure was detected. *String:* ‘Self test failed: $*s*.’ ($*s* is the contents of devSelfTestResult.)
enterpriseTestStart(5)	For physical interfaces and frame relay links: ■ ifIndex (RFC 1573) ■ .0.0 (placeholder) ■ devLastTrapString (devHealthAndStatus.mib For virtual circuits (DLCIs): ■ devFrExtDlciIfIndex (devFrExt.mib) ■ devFrExtDlciDlci (devFrExt.mib) ■ devLastTrapString (devHealthAndStatus.mib	At least one test has been started on an interface or virtual circuit. *String:* ‘$testString test started on $ifString.’ (e.g., ‘DTE Loopback test started on Sync Data Port S01P1.’)
enterpriseTestStop(105)		All tests have been halted on an interface or virtual circuit. *String:* ‘$testString test stopped on $ifString.’ (e.g., ‘Disruptive PVC Loopback test stopped on DLCI 100 of Sync Data Port S01P1 frame relay.’)

Traps: RMON-Specific

Two traps are defined to support the Alarm and Events Groups of RMON. See *RMON Alarm and Event Defaults* on page B-18 for the default values that will generate RMON-specific traps.

Table B-8. RMON-Specific Traps and Variable-Bindings

Trap	Variable-Bindings	Possible Cause
risingAlarm	■ alarmIndex (RFC 1757) ■ alarmVariable (RFC 1757) ■ alarmSampleType (RFC 1757) ■ alarmValue (RFC 1757) ■ alarmRisingThreshold (RFC 1757) ■ devLastTrapString (devHealthAndStatus.-mib)	Object being monitored has risen above the set threshold. *String:* 'Change in $variableName $typeString threshold of $alarmRisingThreshold by $(alarmValue – AlarmRisingThreshold.' (e.g., Octets received on Network T1 frame relay rose to threshold of 1.')
fallingAlarm	■ alarmIndex (RFC 1757) ■ alarmVariable (RFC 1757) ■ alarmSampleType (RFC 1757) ■ alarmValue (RFC 1757) ■ alarmFallingThreshold (RFC 1757) ■ devLastTrapString (devHealthAndStatus.-mib)	Object being monitored has fallen below the set threshold. *String:* 'Change in $variableName $typeString threshold of $alarmFallingThreshold by $(alarmValue – AlarmFallingThreshold.' (e.g., Octets received on Network T1 frame relay fell to threshold of 1.')

Trap: dialControl

These traps indicate when an ISDN backup call is initiated or terminated, or when an outgoing call is rejected by the far end device.

Table B-9. dialControl Traps (1 of 2)

Trap	**Variable-Bindings**	**Possible Cause**
Standard Dial Control MIB		
dialCtlPeerCall-Information	■ callHistoryPeerId (RFC 2128) ■ callHistoryPeerIfIndex (RFC 2128) ■ callHistoryLogicalIfIndex (RFC 2128) ■ ifOperStatus (RFC 1573) ■ callHistoryPeerAddress (RFC 2128) ■ callHistorySubAddress (RFC 2128) ■ callHistoryDisconnect-Cause (RFC 2128) ■ callHistoryConnectTime (RFC 2128) ■ callHistoryDisconnect-Time (RFC 2128) ■ callHistoryInfoType (RFC 2128) ■ callHistoryCallOrigin (RFC 2128)	A peer-to-peer call has been ended. *String:* ‘Call sequence on $ifString *[using B-Chnl $channel]* terminated due to $causeString.’ The B-channel in this example is only provided if it is known. See Most Recent and Previous Cause Values,Table 7-13, DBM Interface Status, in Chapter 7, *Operation and Maintenance*, for a list of the $causeStrings and their cause numbers.
dialCtlPeerCall-Setup	■ callActivePeerId (RFC 2128) ■ callActivePeerIfIndex (RFC 2128) ■ callActiveLogicalIfIndex (RFC 2128) ■ ifOperStatus (RFC 1573) ■ callActivePeerAddress (RFC 2128) ■ callActiveSubAddress (RFC 2128) ■ callActiveInfoType (RFC 2128) ■ callActiveCallOrigin (RFC 2128)	A peer-to-peer call has been sent or received. *String:* ‘Call sequence on $ifString *[using B-Chnl $channel]* initiated *[remotely/locally]*.’ The B-channel in this example is only provided if it is known.

Table B-9. dialControl Traps (2 of 2)

Trap	Variable-Bindings	Possible Cause
Dial Control Extension MIB		
dialCtlPeerCall-Rejected	■ callHistoryPeerId (RFC 2128) ■ callHistoryPeerIfIndex (RFC 2128) ■ callHistoryLogicalIfIndex (RFC 2128) ■ callHistoryPeerAddress (RFC 2128) ■ devLastTrapString (devHealthAndStatus.-mib)	A peer-to-peer call was not successful; the call was rejected by the far end. ■ ISDN Call Profile has been disabled. ■ This unit's phone number was not in the far end device's ISDN Call Profile. *String:* 'Call on $ifString using B-Chnl $channel rejected by remote.'

RMON Alarm and Event Defaults

The FrameSaver unit supports automatic generation of RMON alarm and event information. Each alarm sets an SNMP variable to monitor. When the threshold set for the monitored variable is exceeded, an SNMP trap or a log event is sent.

Event Defaults

Since all events sent are under the control of the FrameSaver unit, there is no need to define multiple events for each alarm type, so only the following two events need to be generated:

eventIndex	eventDescription	eventType	eventCommunity
65533	Default SLV Rising Event	log-and-trap(4)	0
65534	Default SLV Falling Event	log-and-trap(4)	0

The alarm default tables starting on the next page show how each RMON default alarm is set by the FrameSaver unit, shows the alarm and event types, the interval used when generating alarms, and thresholds.

- *Physical Interface Alarm Defaults*
- *Frame Relay Link Alarm Defaults*
- *DLCI Alarm Defaults – Paradyne Area*
- *DLCI Alarm Defaults – NetScout Area*

See *Standards Compliance for SNMP Traps* on page B-8 for information about how traps work, and *Traps: RMON-Specific* on page B-16 for traps specific to remote monitoring.

Rising Event Operation

If a rising threshold is crossed during the interval shown in a table (e.g., frames dropped by the network), the event is armed and an alarm is generated at the end of the interval. Only one alarm per event per interval is generated. The alarm condition persists until the event has been disarmed (reset).

The event is disarmed when a falling threshold has been crossed and the rising threshold has not been crossed during an interval, allowing the event to return to its original disarmed state.

Physical Interface Alarm Defaults

This alarm only applies to the FrameSaver unit's network interface.

Table B-10. Network Physical Interface Alarm Defaults

Item	Sample Type[1]	MIB/Tag/OID[2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Unavailable Seconds	D	*MIB:* DS1/E1 MIB (RFC 1406) *Tag:* dsx1TotalUASs *OID:* .1.3.6.1.2.1.10.18.9.1.5.**I**	900 secs (15 mins)	Rising	1	1

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.

Frame Relay Link Alarm Defaults

These alarms apply to the FrameSaver unit's frame relay link interfaces. They are created during RMON initialization.

Table B-11. Frame Relay Link Alarm Defaults (1 of 2)

Item	Sample Type [1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Invalid Frames	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxIlFrames *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.18.**I**	900 secs (15 mins)	Rising	1	1
Short Frames	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxShort *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.6.**I**	900 secs (15 mins)	Rising	1	1
Long Frames	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxLong *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.7.**I**	900 secs (15 mins)	Rising	1	1
Rx Discards	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxDiscards *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.15.**I**	900 secs (15 mins)	Rising	1	1
Tx Discards	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTxDiscards *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.14.**I**	900 secs (15 mins)	Rising	1	1
Rx Total Errors	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotRxErrs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.20.**I**	900 secs (15 mins)	Rising	1	1

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.

Table B-11. Frame Relay Link Alarm Defaults (2 of 2)

Item	Sample Type[1]	MIB/Tag/OID[2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Tx Total Errors	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotTxErrs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.19.**I**	900 secs (15 mins)	Rising	1	1
Rx Overruns	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxOverruns *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.28.**I**	900 secs (15 mins)	Rising	1	1
Tx Underruns	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTxUnderruns *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.29.**I**	900 secs (15 mins)	Rising	1	1
Rx Non-octet Aligns	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxNonOctet *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.16.**I**	900 secs (15 mins)	Rising	1	1
Rx CRC Errors	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxCrcErr *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.17.**I**	900 secs (15 mins)	Rising	1	1
Total LMI Errors	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotalLMIErrs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.32.**I**	900 secs (15 mins)	Rising	1	1

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.

DLCI Alarm Defaults – Paradyne Area

These alarms apply to all DLCIs on the network interface and can be created during RMON initialization or when a DLCI is created. They are put into the Paradyne-defined alarm area.

Table B-12. DLCI Alarm Defaults – Paradyne Area (1 of 2)

Item	Sample Type[1]	MIB/Tag/OID[2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
DLCI Inactive Seconds	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsInactive-Secs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.2.**I.D**	900 secs (15 mins)	Rising	1	1
Missing Latency Responses	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciMissedSLVs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.23.**I.D**	900 secs (15 mins)	Rising	5	5
Rx FECNs	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs *OID:* .1.3.6.1.2.1.10.32.2.1.4.**I.D**	60 secs (1 min)	Rising	1	1
Rx BECNs	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs *OID:* .1.3.6.1.2.1.10.32.2.1.5.**I.D**	60 secs (1 min)	Rising	1	1
Congested Seconds	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciSts-CongestedSecs *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.2.1.6.**I.D**	60 secs (1 min)	Rising	5	5
Frames Dropped by Network	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciNetDropFr *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.20.**I.D**	60 secs (1 min)	Rising	1	1

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.
D = DLCI number.

Table B-12. DLCI Alarm Defaults – Paradyne Area (2 of 2)

Item	Sample Type[1]	MIB/Tag/OID[2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Maximum Latency	A	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyMax *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.**I**.**D**	60 secs (1 min)	Rising	0	0

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.
D = DLCI number.

DLCI Alarm Defaults – NetScout Area

These alarms can be created during RMON initialization or when a DLCI is created. They are put into the NetScout alarm area. Table B-11 identifies alarm defaults that do not change, and Table B-13, Static DLCI Alarm Defaults – NetScout Area identifies alarm defaults that change when the interface's line speed changes.

The thresholds for these alarms can be edited using NetScout Manager Plus so they match the values in the SLA between the customer and service provider. Up to eight alarms per interface are allowed. Any additional alarms are added to the Paradyne Area alarms and they cannot be changed using NetScout software.

See *Editing Alarms* in Chapter 10, *Setting Up NetScout Manager Plus for FrameSaver Devices*.

Table B-13. Static DLCI Alarm Defaults – NetScout Area

Item	Sample Type[1]	MIB/Tag/OID [2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Current Latency	A	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyLatest *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.7.**I**.**D**	60 secs (1 min)	None	Must be configured.	0
Average Latency	A	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyAvg *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.3.1.5.**I**.**D**	900 secs (15 mins)	None	Must be configured.	0
Frames Received	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames *OID:* .1.3.6.1.2.1.10.32.2.1.8.**I**.**D**	60 secs (1 min)	None	Must be configured.	0
Frames Sent	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames *OID:* .1.3.6.1.2.1.10.32.2.1.6.**I**.**D**	60 secs (1 min)	None	Must be configured.	0
Tx Frames Exceeding CIR	D	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciTxFrOutCIR *OID:* .1.3.6.1.4.1.1795.2.24.2.6.9.4.1.1.17.**I**.**D**	60 secs (1 min)	None	Must be configured.	0
Tx CIR Utilization	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets *OID:* .1.3.6.1.2.1.10.32.2.1.7.**I**.**D**	60 secs (1 min)	None	Must be configured.	0

[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.
D = DLCI number.

Table B-14. Dynamic DLCI Alarm Defaults – NetScout Area

Item	Sample Type[1]	MIB/Tag/OID[2]	Interval	Event Type	Rising Threshold Default	Falling Threshold Default
Rx DLCI Link Utilization	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets *OID:* .1.3.6.1.2.1.10.32.2.1.9.**I**.**D**	60 secs. (1 min)	Rising	70% of link capability	65% of link capability
Tx DLCI Link Utilization	D	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets *OID:* .1.3.6.1.2.1.10.32.2.1.7.**I**.**D**	60 secs. (1 min)	Rising	70% of link capability	65% of link capability

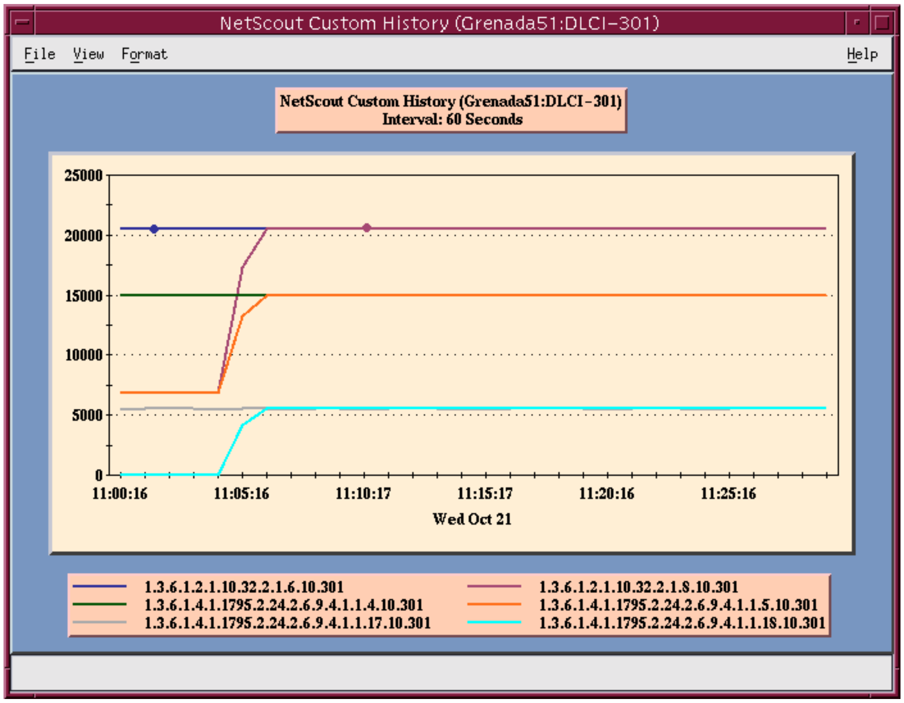
[1] D = Delta. Indicates that the calculated difference between the current value and the previous value is contained in the MIB.
A = Absolute. Indicates that the exact value for the item is contained in the MIB.

[2] **I** in the OID = Interface ID of the frame relay link.
D = DLCI number.

Object ID Cross-References (Numeric Order)

The FrameSaver unit supports automatic generation of RMON alarm and event information. Each alarm sets an SNMP variable to monitor. When the threshold set for the monitored variable is exceeded, an SNMP trap or a log event is sent.

This table is helpful in identifying alarm conditions being tracked when viewing the NetScout Custom History screen (shown below), which provides the OID instead of the alarm condition.



See Table B-15, History OID Cross-Reference, for an RMON history OID cross-reference and Table B-16, Alarm OID Cross-Reference, for an RMON alarm OID cross-reference.

Table B-15. History OID Cross-Reference (1 of 5)

Object ID (OID)[1]	Item	MIB/Tag
.1.3.6.1.2.1.2.2.1. . .		
.1.3.6.1.2.1.2.2.1.**5.I**	Link Speed	*MIB:* MIB II (RFC 1573) *Tag:*ifSpeed
.1.3.6.1.2.1.2.2.1.**10.I**	All DLCI + LMI Rx Octets	*MIB:* MIB II (RFC 1573) *Tag:*ifInOctets
.1.3.6.1.2.1.2.2.1.**16.I**	All DLCI + LMI Tx Octets	*MIB:* MIB II (RFC 1573) *Tag:*ifOutOctets
.1.3.6.1.2.1.2.10.32.2.1. . .		
.1.3.6.1.2.1.10.32.2.1.4.**I.D**	Rx FECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:*frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I.D**	Rx BECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I.D**	Tx Frames	*MIB:* FR DTE MIB (RFC 2115) *Tag:*frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx Octets	*MIB:* FR DTE MIB (RFC 2115) *Tag:*frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I.D**	Rx Frames	*MIB:* FR DTE MIB (RFC 2115) *Tag:*frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I.D**	Rx Octets	*MIB:* FR DTE MIB (RFC 2115) *Tag:*frCircuitReceivedOctets
.1.3.6.1.2.1.16.12.2.1. . .		
.1.3.6.1.2.1.16.12.2.1.**2.P**	Protocol Octets (for 11 protocols)	*MIB:* RMON II (RFC 2021) *Tag:*protocolDistStatsOctets

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-15. History OID Cross-Reference (2 of 5)

Object ID (OID)[1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2. . .		
.1.3.6.1.4.1.1795.2.24.2.**6.5.4.8.1.2.I**	Unavailable Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:*devFreeRunUAS
.1.3.6.1.4.1.1795.2.24.2.**6.9.4.7.1.16.I**	Rx Non-octet Aligns	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtLinkRxNonOctet
.1.3.6.1.4.1.1795.2.24.2.**13.1.2.1.4.H.T.N**	IP Top Listeners (1–6)	*MIB:* pdn_FrExt.mib (E) *Tag:*devRmonIPTopNDstIP
.1.3.6.1.4.1.1795.2.24.2.**13.1.2.1.6.H.T.N**	IP Top Talkers (1–6)	*MIB:* pdn_FrExt.mib (E) *Tag:*devRmonIPTopNSrcIP
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.3.I.D**	DLCI CIR	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciFrCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.7.I.D**	Tx DEs	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciTxDE
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.8.I.D**	Tx BECNs	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrCircuitTxBECN
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.17.I.D**	Tx Frames Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciTxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.18.I.D**	Rx Frames Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciRxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.20.I.D**	Network Frames Lost	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.22.I.D**	Rx DEs	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciRxDE
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.37.I.D**	Network Frames Offered	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciRmtOffFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.39.I.D**	Network Frames Offered In CIR	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciRmtOffFrInCir

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-15. History OID Cross-Reference (3 of 5)

Object ID (OID)[1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.41.I.D**	Network Frames Dropped In CIR	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciDropOffFrInCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.43.I.D**	Network Frames Offered Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciRmtOffFrOutCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.45.I.D**	Network Frames Lost Above CIR	*MIB:* pdn_FrExt.mib (E) *Tag:*devFrExtDlciRmtDropFrOutCir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.55.I.D**	Network Frames Offered Above CIR Within EIR	*MIB:* pdn_FrExt.mib (E) *Tag*:devFrExtDlciDropFrCirToEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.57.I.D**	Network Frames Dropped Above CIR Within EIR	*MIB:* pdn_FrExt.mib (E) *Tag*:devFrExtDlciRxFrNetDropCirToEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.59.I.D**	Network Frames Offered Above EIR	*MIB:* pdn_FrExt.mib (E) *Tag*:devFrExtDlciOfferedFrOverEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.61.I.D**	Network Frames Dropped Above EIR	*MIB:* pdn_FrExt.mib (E) *Tag*:devFrExtDlciRxFrNetDropOverEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.63.I.D**	DLCI EIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciEir
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.2.I.D**	DLCI Inactive Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsInactiveSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.8.I.D**	Backup Count	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsBackupCnt
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.9.I.D**	Backup Time	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsBackupTime
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.5.I.D**	Average Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.6.I.D**	Maximum Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyMax

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-15. History OID Cross-Reference (4 of 5)

Object ID (OID) [1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.8.I.D**	Latency Packet Size	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyPacketSz
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2 . . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2.**1.2.I.N**	Frame Size Upper Limit (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtFrameSzUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.2.**1.3.I.N**	Frame Size Count (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtFrameSzCount
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1**.2.I.D.N**	Burst Upper Limit (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtBurstUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1**.3.I.D.N**	Burst Octets (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtBurstOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4.5.2.1**.4.I.D.N**	Burst Frames (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtBurstFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**2.I**	LMI Unavailable Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkNoLMISecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**6.I**	Rx Short Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**7.I**	Rx Long Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**11.I**	LMI Sequence Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkSeqErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**15.I**	Rx Discards	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**17.I**	Total Rx CRC Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxCrcErr

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

Table B-15. History OID Cross-Reference (5 of 5)

Object ID (OID)[1]	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**18.I**	Rx Illegal Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxIlFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**19.I**	Total Tx Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**20.I**	Total Rx Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.7.1.**32.I**	Total LMI Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotLMIErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1.**2.I.N**	Port Burst Upper Limits (1–4)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkUtilUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1.**3.I.N**	Rx Port Burst Octets (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkUtilRxOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4.10.3.1.**4.I.N**	Tx Port Burst Octets (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkUtilTxOctets

[1] **I** = Interface ID of the frame relay link
D = DLCI number
N = Additional numeric index used by tables, like frame or burst size
H = Host control index
P = Protocol index
T = The time mask

See Table B-16, Alarm OID Cross-Reference for an RMON alarm OID cross-reference.

Table B-16. Alarm OID Cross-Reference (1 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.2.1.10.18.9.1. . .		
.1.3.6.1.2.1.10.18.9.1.**5.I**	Unavailable Seconds	*MIB:* DS1/E1 MIB (RFC 1406) *Tag:* dsx1TotalUASs
.1.3.6.1.2.1.10.32.2.1. . .		
.1.3.6.1.2.1.10.32.2.1.**4.I.D**	Rx FECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFECNs
.1.3.6.1.2.1.10.32.2.1.**5.I.D**	Rx BECNs	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedBECNs
.1.3.6.1.2.1.10.32.2.1.**6.I.D**	Frames Sent	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentFrames
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx CIR Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**7.I.D**	Tx DLCI Link Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitSentOctets
.1.3.6.1.2.1.10.32.2.1.**8.I.D**	Frames Received	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedFrames
.1.3.6.1.2.1.10.32.2.1.**9.I.D**	Rx DLCI Link Utilization	*MIB:* FR DTE MIB (RFC 2115) *Tag:* frCircuitReceivedOctets
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.17.I.D**	Tx Frames Exceeding CIR	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciTxFrOutCIR
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.20.I.D**	Frames Dropped by Network	*MIB:* pdn_FrExt.mib (E) *Tag:* frFrExtDlciNetDropFr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**1.1.23.I.D**	Missing Latency Responses	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciMissedSLVs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.6.I.D**	Congested Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsCongestedSecs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**2.1.2.I.D**	DLCI Inactive Seconds	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtDlciStsInactiveSecs

[1] **I** = Interface ID of the frame relay link
D = DLCI number

Table B-16. Alarm OID Cross-Reference (2 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.5.I.D**	Average Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyAvg
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**3.1.7.I.D**	Current Latency	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLatencyLatest
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.**2.1.2.I.N**	Frame Size Upper Limits (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtFrameSzUpLimit
.1.3.6.1.4.1.1795.2.24.2.6.9.4.4.**2.1.3.I.N**	Frame Size Count (1–5)	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtFrameSzCount
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.6.I**	Rx Short Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxShort
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.7.I**	Rx Long Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxLong
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.11.I**	LMI Sequence Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkSeqErr
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.14.I**	Tx Discards	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.15.I**	Rx Discards	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxDiscards
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.16.I**	Rx Nonoctet Aligns	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxNonOctet
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.17.I**	Rx CRC Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxCrcErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.18.I**	Rx Illegal Frames	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxIlFrames
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.19.I**	Tx Total Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotTxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.20.I**	Rx Total Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotRxErrs
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.28.I**	Rx Overruns	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkRxOverruns

[1] **I** = Interface ID of the frame relay link
D = DLCI number

Table B-16. Alarm OID Cross-Reference (3 of 3)

Object ID (OID)	Item	MIB/Tag
.1.3.6.1.4.1.1795.2.24.2.6.9.4. . .		
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.29.I**	Tx Underruns	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTxUnderruns
.1.3.6.1.4.1.1795.2.24.2.6.9.4.**7.1.32.I**	Total LMI Errors	*MIB:* pdn_FrExt.mib (E) *Tag:* devFrExtLinkTotalLMIErrs

[1] **I** = Interface ID of the frame relay link
D = DLCI number

Router CLI Commands, Codes, and Designations

C

CLI Commands

The FrameSaver SLV 9126-II Router is managed with text commands from the Command Line Interface (CLI). The CLI can be accessed:

- Locally via a PC or asynchronous terminal connected to the COM port.
- Remotely via a Telnet session.

The conventions used in the command line syntax are shown below.

Convention	Meaning
[ ]	Brackets indicate an optional element.
{ }	Braces indicate a required entry.
|	Vertical bars separate mutually exclusive elements. Enter one element only.
[{ }]	Braces within brackets indicate a required choice within an optional element.
Italics	The entry is a variable.
`Courier Bold`	The entry in its explicit form is typed as shown. (Most commands can be abbreviated. See the *FrameSaver SLV 9126-II Router Quick Reference* for more information.)
x.x.x.x	32-bit IP address and mask information where *x* is an 8-bit weighted decimal notation.
xx:xx:xx:xx:xx:xx	MAC address information where *x* is a hexadecimal notation.

With the exception to the Login ID and Password, the CLI is not case-sensitive.

Refer to *Navigating the Router's CLI* in Chapter 2, *User Interface and Basic Operation,* for additional information.

This appendix contains the following tables for commands:

- Table C-1, Pager Command
- Table C-2, Access Control Commands
- Table C-3, Configuration Commands
- Table C-4, Interface Commands
- Table C-5, IP Routing Commands
- Table C-6, Bridge Commands
- Table C-7, ARP Commands
- Table C-8, NAT Commands
- Table C-9, DHCP Server Commands
- Table C-10, DHCP Relay Agent Commands
- Table C-11, Filter Commands
- Table C-12, Diagnostic Commands
- Table C-13, Show Commands

In addition, the following tables are used in the commands above.

- Table C-14, Ethernet Type Codes (Hex)
- Protocol and Port Designations
  - Table C-15, ICMP Designations
  - Table C-16, TCP Port Designations
  - Table C-17, UDP Port Designations

Pager Command

The pager command allows you to enable or disable screen paging for a CLI session, and enter comments at the command line, which is useful when adding comments within scripts.

Table C-1. Pager Command

[no] **pager**
Minimum Access Level modes: **Operator** Command Mode: **All modes**
Allows you to control the flow of uninterrupted output to the screen. Information added after the **!** at the command line is ignored. **pager** – Enables display paging. When enabled and there are more than 23 lines to display, **`more`** displays on line 24. This is the default each time a session is started. – Press the Spacebar to view the next screen. – Press the Enter key to display the next line. – Press the **q** key, **Ctrl-c**, or any other key to return to the command line. **no pager** – Disables paging, and the entire output is sent to the screen without interruption.

Access Control Commands

Access control commands allow you to end a session. For password and changing access commands, see Chapter 6, *Security and Logins*.

Table C-2. Access Control Commands

end
Minimum Access Level: **Administrator** Command Mode: **All config modes**
Allows you to exit any configuration mode and return to standard operating mode.
exit
Minimum Access Level: **Operator** Command Mode: **All modes**
Allows you to exit the current mode or end the session. If configuration changes have been made when **exit** is entered, the **`There are unsaved configuration changes. Are you sure you want to exit? (no, yes)`** prompt appears. – If **yes** is entered, the router leaves configuration mode and any configuration changes are lost. – If **no** is entered, the configuration prompt is returned to so you can save your changes. If in standard operating mode when **exit** is entered, the session is ended and you are returned to the Main Menu.

Configuration Commands

Configuration control commands put the router in configuration mode and allows you to save configuration changes. To show a configuration, see Table C-13, Show Commands.

Table C-3. Configuration Commands

**`configure {terminal	factory}`**
Minimum Access Level: **Administrator** Command Mode: **config**
Causes the router to enter configuration mode. The router stays in configuration mode until the **`exit`** command is entered or the session times out. Example: **`configure terminal`** NOTES: When in configuration mode: – SNMP **`set`** commands or changes saved from the menu-driven user interface for router configuration are prevented; an in use message is generated. – Router sub-interfaces and/or DLCIs cannot be added or deleted via the menu-driven user interface's CreatePVC function key. – The number of configuration commands that can be entered without performing a **`save`** is limited; a warning message is generated. – The only **`show`** command available is **`show configuration`**. **terminal** – Enter configuration mode and a copy of the currently running configuration is loaded into the edit buffer. Any changes made in the buffer overwrite the copied current configuration when the **`save`** command is entered, the configuration is saved to the currently running configuration (terminal), and an automatic reset is performed. **factory** – Enter configuration mode and a copy of the factory default settings is loaded into the edit buffer. Any changes made in the buffer overwrite the copied default settings when the **`save`** command is entered, the configuration is saved to the currently running configuration (terminal), and an automatic reset is performed. This is the default.
`save`
Minimum Access Level: **Administrator** Command Mode: **All config modes**
Causes configuration changes to be saved to the currently active configuration, and the router to be reset. If the **`save`** command is entered and changes made require a reboot of the device, a prompt states that a reset is required for the changes to take effect. – If **yes** is entered, changes are stored and the device resets automatically. A message displays when the save is complete. – If **no** is entered, you stay in configuration mode.

Interface Commands

Interface commands allow you to configure the Ethernet and network interfaces, and their sub-interfaces.

Table C-4. Interface Commands (1 of 3)

`interface` *intf-type intf-num* **`no interface`** *intf-type intf-num.sub-intf-num* **`[point-to-point]`**
Minimum Access Level: **Administrator** Command Mode: **config, config-if, config-subif**
Allows you to enter interface or sub-interface configuration mode and create sub-interfaces. All commands entered while in interface or sub-interface configuration mode are applied to the specified interface or sub-interface. No sub-interfaces are enabled by default. Example: **`interface serial 132.53.4.2 132.53.4.250`** Use the **`no interface`** command to delete sub-interfaces while in **config** mode. The command does not delete interfaces. When a sub-interface that is currently in use is deleted, all sub-interface uses are automatically removed from the system configuration. This includes all route entries destined for the sub-interface; ip addresses and subnets for the sub-interface; and all frame relay DLCIs, bridge group assignments, and ip nat inside/outside assignments configured on the sub-interface. ***intf-type*** – Serial interface is supported, the frame relay serial interface. ***intf-num*** – Interface index number for the Serial interface. Valid range is from 0 up to the maximum number of serial interfaces, minus one. ***sub-intf-num*** – Sub-interfaces are only supported on the network interface (Serial 0). Valid range for the sub-interface is 0–4,294,967,295. **point-to-point** – Specifies a point-to-point sub-interface. By default, all sub-interfaces are point-to-point.

Table C-4. Interface Commands (2 of 3)

`ip address` *ip-addr subnet-mask*

`no ip address` **[***ip-addr subnet-mask***]**

Minimum Access Level: **Administrator**
Command Mode: **config-if** (Ethernet), **config-subif** (Serial)

Assigns an IP address to the Ethernet interface or a Serial port sub-interface. No IP addresses are assigned to interfaces or sub-interfaces by default.

Example: **`ip address 132.53.4.2 255.255.255.255`**

Use the **`no ip address`** command to remove an IP address assigned to an interface or sub-interface, and disable IP processing on the interface. The following rules apply:

- Each sub-interface must be assigned to a different subnet.
- A customer data IP address and subnet mask must be different from any IP address used for management.
- When an IP address and subnet mask are assigned to an interface or sub-interface, the device automatically creates a routing table entry with the same destination address and subnet mask, saying that IP addresses within that range are directly reachable on the interface. This is the *interface route*.
- If the maximum number of static routes have already been configured, you cannot assign an IP address to the interface or sub-interface.
- When an interface address and subnet mask are deleted, any routing entries with a Next Hop Router address that fall within the interface's address range are deleted automatically.

ip-address – IP address of the interface or sub-interface.

subnet-mask – Subnet mask to be used when the IP address is being compared during route table lookups. The subnet mask cannot be 0.0.0.0 and only contiguous, left-justified subnet masks are allowed.

`encapsulation` *encapsulation-type encapsulation-protocol*

Minimum Access Level: **Administrator**
Command Mode: **config-if** (Serial)

Specifies the type of encapsulation on an interface.

Example: **`encapsulation frame-relay ietf`**

encapsulation-type – Specifies Frame Relay encapsulation on the serial interface. The default is **frame-relay**.

encapsulation-protocol – Specifies RFC 1490 encapsulation protocol on the serial interface. The default is **ietf**.

Table C-4. Interface Commands (3 of 3)

[no] `ip unnumbered` [`null 0`]
Minimum Access Level: **Administrator** Command Mode: **config-subif**
Enables or disables IP processing on a serial sub-interface without assigning an explicit address. The **`no ip unnumbered`** command removes any IP address assigned to the interface and disables IP processing on the interface. The default is that IP processing is disabled. Example: **`ip unnumbered`** When an interface IP address and subnet mask are deleted via the **no ip unnumbered** command, any routing entries with a Next Hop Router address that fall within the interface's address range are deleted automatically.
[no] `frame-relay interface-dlci` *dlci-num*
Minimum Access Level: **Administrator** Command Mode: **config-subif**
Specifies or removes a DLCI on a sub-interface configured for frame relay encapsulation. Only one DLCI may be configured per sub-interface. Example: **`frame-relay interface-dlci 103`** ***dlci-num*** – Any valid DLCI number that is not already in use on the interface. Range for DLCI numbers is 16–1007. The default is None.

IP Routing Commands

Internet Protocol (IP) routing commands are used to enable and disable IP routing, and to create or delete static routes in the routing table.

To show IP routing and performance statistics, see Table C-13, Show Commands.

Table C-5. IP Routing Commands

ip route *dest-ip dest-mask* **{***next-hop-ip* **|** *intf-type intf-num* **[.***sub-intf-num***] }** **no ip route** *dest-ip dest-mask* **[***next-hop-ip* **|** *intf-type intf-num* **[.***sub-intf-num***]]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows manual creation or deletion of static route entries. There are no route entries by default. A default gateway destination route may be specified by entering a destination IP address and mask of “0.0.0.0 0.0.0.0” with a default gateway IP address or interface. Example: **ip route 132.53.4.2 255.255.255.255 serial 0.*x*** NOTE: Generally, routes are specified using a next hop address. However, routes over unnumbered point-to-point sub-interfaces should specify the sub-interface to reach the destination. ***dest-ip*** – IP address of the destination host or network or “0.0.0.0” if a default destination gateway is specified. ***dest-mask*** – The subnet mask to be used when the destination IP address is compared during route table lookups. The dest-mask cannot be 0.0.0.0 unless a dest-ip address of 0.0.0.0 has been specified, and only contiguous, left-justified masks are allowed. ***next-hop-ip*** – IP address of the next-hop router used to reach the destination. ***intf-type*** – Two interface types are supported: – **Ethernet** – IEEE 802.3 interface – **Serial** – Frame relay serial interface ***intf-num*** – Valid interface index number for both the Ethernet and Serial interfaces is **0**. ***sub-intf-num*** – Sub-interfaces are only supported on the network interface (Serial 0). If a serial interface is specified, a sub-interface must also be specified. Valid range for a sub-interface is 0–4,294,967,295.
[no] ip routing
Minimum Access Level: **Administrator** Command Mode: **config**
Enables or disables IP routing in the device. The IP routing default is Enable. NOTE: When IP routing is disabled, all static route entries are deleted. However, adding new route entries while IP routing is disabled is not prevented.
[no] ip multicast-routing
Minimum Access Level: **Administrator** Command Mode: **config**
Enables or disables the forwarding of IP multicast packets. The default is Disable.

Bridge Commands

Bridge commands are used to enable or disable simultaneous bridging and routing, configuration of bridge groups and their attributes, and apply or remove bridge groups from an interface or sub-interface.

To show the bridge database or spanning-tree topology, see Table C-13, Show Commands.

Table C-6. Bridge Commands (1 of 2)

bridge {crb | *bridge-group* **{acquire | aging-time** *aging-time* **|**
protocol *span-tree-protocol* **| priority** *span-tree-priority* **|**
route *route-protocol***}}**

no bridge {crb | *bridge-group* **{acquire | aging-time[***aging-time***] |**
priority[*span-tree-priority***] | route [***route-protocol***] }}**

Minimum Access Level: **Administrator**
Command Mode: **config**

A user can enable or disable simultaneous bridging and routing and configure attributes associated with a bridging group. Bridge group 1 is created by default with a priority of 32768 and configured as a learning bridge utilizing the IEEE 802.1 spanning tree protocol.

Simultaneous routing and bridging is disabled by default. Once concurrent routing/bridging is enabled, you must configure an explicit bridge route for any protocol to be routed on interfaces in a bridge group.

Example: **bridge crb 1 route ip**

crb – Enable or disable concurrent routing and bridging on the device.

bridge-group – Bridge group 1 is created by default. If a bridge-group is specified, one of the following attributes **must** be specified:

acquire – Configure a learning bridge that is capable of dynamically learning new stations. This argument is configured by default on all bridge groups. The **no bridge** command is not accepted for this argument.

aging-time – Specifies the length of time that an unused dynamic entry is maintained in the bridge table. The **no bridge** command resets the aging-time to the default value.

aging-time – Valid range is 10–1,000,000 seconds. The default is 300.

protocol – Specify a spanning tree protocol.

span-tree-protocol – Valid spanning tree protocol for IEEE 802.1 protocol is ieee.

priority – Specify the priority ranking for this bridge. The higher the number, the less likely this bridge will be selected as the spanning tree root.

span-tree-priority – Valid priority values when spanning tree protocol is IEEE.802.1 are: 0–65535. The default is 32768.

route – Specify a protocol to be routed in this bridge group when concurrent routing and bridging are enabled.

route-protocol – Valid routing protocol is IP.

Table C-6. Bridge Commands (2 of 2)

[no] `bridge-group` *bridge-group*

Minimum Access Level: **Administrator**
Command Mode: **config-if, config-subif**

Allows a user to apply or remove a set of bridge group parameters to/from an interface or sub-interface. When a set of bridge group parameters is applied or removed at the interface level, the command also applies to all sub-interfaces on the interface.

Example: **`no bridge-group`**

NOTE: If the bridge group is only required on specific sub-interfaces, remove the bridge group from an interface and apply it at the sub-interface level.

bridge-group – Valid bridge group number **1** is applied to all interfaces by default. Any sub-interfaces created on interfaces where the bridge group is applied inherit the bridge group.

[no] `bridge-group` *bridge-group*
{`input-type-list` *in-access-list-200num* **|**
`output-type-list` *out-access-list-200num***}**

Minimum Access Level: **Administrator**
Command Mode: **config-if**

Allows a user to specify or remove an input or output Ethernet type code filter for an interface. No bridge group filters are applied to interfaces by default.

Example: **`bridge-group 1 input-type-list 8069`**

NOTE: The order in which access-list filters are entered affects the order in which the filters are applied. Each filter is applied in succession until all filters have been applied. If no conditions match, a frame is discarded.

bridge-group – Valid bridge group number **1** is applied to all interfaces by default. Any sub-interfaces created on interfaces where the bridge group is applied inherit the bridge group.

input-type-list – Specify the filter applied to incoming Ethernet packets by type code. Refer to Table C-14, Ethernet Type Codes (Hex).

in-access-list-200num – The input type access list valid range for protocol type-code access lists: 200–299.

output-type-list – Specify the filter applied to outgoing Ethernet packets by type code. Refer to Table C-14, Ethernet Type Codes (Hex), Ethernet Type Codes (Hex).

out-access-list-200num – The output type access list number valid range for protocol type-code access lists: 200–299.

ARP Commands

Address Resolution Protocol (ARP) commands are used to create entries in the ARP table, specify how long the information will be retained, and remove dynamic entries in the table.

Table C-7. ARP Commands

arp *ip-address mac-address arp-type* **no arp** *ip-address* **[***mac-address arp-type***]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to create or delete a single, static ARP table entry. Static ARP entries created with this command are permanent and are retained across resets/power cycles. Up to the maximum number of static ARP entries specified may be entered. There are no static ARP entries by default. ***ip-address*** – The IP address of the ARP entry to be created or deleted. ***mac-address*** – MAC address. ***arp-type*** – Specifies the ARP type. Valid ARP type is **arpa**, the standard Ethernet-style ARP (RFC 826).
arp timeout *time* **no arp timeout [***time***]**
Minimum Access Level: **Administrator** Command Mode: **config-if** (Ethernet)
Allows you to specify the amount of time that ARP information is retained in the ARP cache. The **no arp timeout** command restores the default ARP timeout value. Example: **arp timeout 28000** NOTES: – The amount of time the device waits before reattempting to acquire ARP information for incomplete entries is 5 seconds and is not configurable. – The internal ARP timeout timer has one minute precision, so the ARP timeout is implemented by rounding up to the nearest minute. ***time*** – The ARP timeout value in seconds. Valid range is 1–4294967 seconds. The default is 14400.
clear arp-cache
Minimum Access Level: **Administrator** Command Mode: **Standard**
Deletes all dynamic ARP table entries from the ARP cache.

NAT Commands

Network Address Translation (NAT) commands are used to enable or disable NAT on an interface or sub-interface and specify whether IP addresses on the interface are public or private.

Table C-8. NAT Commands (1 of 3)

[no] ip nat {inside | outside}
Minimum Access Level: **Administrator** Command Mode: **config-if, config-subif**
Allows you to specify if Network Address Translation (NAT) is performed on an interface or sub-interface and whether IP addresses on the interface are private or public addresses. NAT is disabled by default. Example: **ip nat inside** **inside** – Specifies inside (private) IP addresses on this interface. **outside** – Specifies outside (public) IP addresses on this interface.
ip nat translation timeout [*time*] **no ip nat translation timeout [*time*]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to specify the amount of time that a dynamically configured standard NAT (non-port translation) mapping can remain unused before the mapping is automatically deleted. The default is 24 hours. To reset the timeout to the default, use the **no nat translation timeout** command. Example: **ip nat translation timeout 604800** NOTE: When NAPT is enabled, mappings are automatically deleted based on a separate set of non-configurable timeouts: – UDP translations timeout: 5 minutes. – TCP translations timeout: 24 hours. – ICMP translations timeout: 1 minute. ***time*** – The timeout value in seconds. The valid range is 1–2147483647. The default is 86400 seconds (24 hours).

Table C-8. NAT Commands (2 of 3)

```
ip nat pool pool-name start-ip-addr end-ip-addr
    {netmask netmask |{prefix-length |/} prefix-length}

no ip nat pool pool-name [start-ip-addr end-ip-addr
    {netmask netmask | {prefix-length |/} prefix-length} ]
```

Minimum Access Level: **Administrator**
Command Mode: **config**

Defines a pool of addresses for Network Address Translation. Addresses can then be allocated from the pool as needed. Up to 30 NAT pools can be supported.

To remove a pool, use the **no ip nat pool** command. No NAT pools are configured by default.

Example: **ip nat pool Largo 132.53.4.2 132.53.4.250 / 24**

pool-name – Name of the pool comprised of 1–20 ASCII printable characters.

start-ip-addr – Starting IP address of the range of addresses in the address pool.

end-ip-addr – Ending IP address of the range of addresses in the address pool.

netmask – Specify a network mask that indicates which address bits belong to the network and subnet fields, and which bits belong to the host field.

netmask – Network mask of the network for the pool addresses.

prefix-length or **/** – Specify the number of bits in a network mask address that are ones and define the network and subnet fields.

prefix-length – The number of bits in a network mask address that are ones. Valid range is 1–32.

```
[no] ip nat inside source
    {list access-list-1-99num pool pool-name [overload] |
    list access-list-1-99num interface intf-type intf-num
        [.sub-intf-num] overload |
    static {static-ip-addr1 static-ip-addr2 |
        protocol static-ip-addr1 static-port-num static-ip-addr2}}
```

Minimum Access Level: **Administrator**
Command Mode: **config**

Allows a user to specify or remove Network Address Translation rules. Both dynamic and static address translations may be specified. Command forms that include an access list are used to specify dynamic translation rules. Packets from addresses that match the access list are translated using addresses allocated from the named pool or the IP address assigned to the interface. No NAT rules are configured by default.

Example: Refer to Chapter 4, *Configuration Options*.

inside – Inside address translation converts an inside (private) IP address to an outside (public) IP address (and port, if overload is specified for NAPT).

source – Specifies source address translation.

list – Specify the access list number for *dynamic* address translation. For inside source translation, this access list describes local addresses. If no rules have been created for the specified access list, no translations based on this rule will occur.

access-list-1-99num – A standard IP Access list. The valid range is 1–99.

(Continued on next page)

Table C-8. NAT Commands (3 of 3)

(Continued from previous page)

pool – Specify the name of a pool of addresses available for dynamic address translation. For inside source translation, this is the pool of local addresses.

> ***pool-name*** – The name of a NAT pool comprised of 1–20 ASCII printable characters.

interface – For dynamic address translation, specifies an interface or sub-interface that provides the address for the translation. For inside source translation, specifies the interface that provides the global address. If there is no address on the interface, the interface has not been specified as an outside interface, or the interface is not operational, no translations based on this rule will occur. If a public IP address is specified for NAPT on this interface, that address is used instead of the interface's assigned IP address.

> ***intf-type*** – Two interface types are supported:
>
> > **Ethernet** – IEEE 802.3 interface
> >
> > **Serial** – Frame relay serial interface
>
> ***intf-num*** – Interface index number for both the Ethernet and Serial interfaces, 0 or 1.
>
> ***sub-intf-num*** – Sub-interface number. Sub-interfaces are only supported on the network interface (Serial 0). If a Serial interface is specified, a sub-interface must also be specified. Sub-interface number range is 0–4,294,967,295.

overload – Specifies that Network Address Port Translation (NAPT), also known as Port Address Translation (PAT), is to be used for UDP and TCP.

static – Specifies a fixed, one-to-one mapping between an inside (private) IP address (and port for PAT) and a outside (global) IP address (and port for PAT). For inside source translation, a private address (and port for PAT) is mapped to a global address (and port for PAT). Static inside and outside destination translations are not supported.

> ***static-ip-addr1*** – Specifies the first IP address in the *static route*. For inside source translation, this is the local address to be mapped.
>
> ***static-ip-addr2*** – Specifies the second IP address in the *static route.* For inside source translation, this is the global address to be mapped.
>
> ***protocol*** – Protocol that applies to this *static* route, which include:
>
> > **tcp** – Transmission Control Protocol
> >
> > **udp** – User Datagram Protocol
>
> ***static-port-num*** – Specifies the second TCP/UDP port in a *static protocol* route. For inside source translation, this is the local port. It should only be specified when a static protocol translation is specified. Only one static route per protocol can specify a *static-port-num*. The valid range of TCP/UDP ports is 1–65535.

```
clear ip nat translation *
```

Minimum Access Level: **Administrator**
Command Mode: **Standard**

Allows you to clear all *dynamic* NAT translations from the translation table.

DHCP Server Commands

Dynamic Host Configuration Protocol (DHCP) server commands are used to enable or disable the DHCP server, and create or delete a DHCP pool.

Table C-9. DHCP Server Commands (1 of 3)

[no] `service dhcp`
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to enable or disable the DHCP server. The DHCP server is enabled by default but is not active until other DHCP server options are configured. When an IP address is assigned to a host by the DHCP Server and there is no matching routing table entry, a host entry for that IP address is created. This entry is deleted from the routing table when the lease expires or the IP address is relinquished. When an IP address is assigned to a host on the local Ethernet by the DHCP Server, an ARP table entry is created mapping that IP address to the corresponding host MAC address. This entry is deleted from the ARP table when the lease expires or the IP address is relinquished. This entry is not deleted according to the timeout mechanism that applies to normal ARP entries. NOTE: The DHCP Relay and DHCP Server cannot be enabled at the same time.
[no] `ip dhcp pool` *pool-name*
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to create or delete a DHCP pool and places it in DHCP pool configuration mode to configure IP DHCP pool parameters. All commands entered while in DHCP pool configuration mode are applied to the specified DHCP pool. No DHCP pools are configured by default. Example: **`ip dhcp pool pool17`** ***pool-name*** – The name of the DHCP pool, as 1–20 ASCII printable characters.
[no] `ip dhcp excluded-address` *ip-addr* **[***end-ip-addr***]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to specify a single IP address, or a range of IP addresses, that the DHCP server should not distribute to clients. The **`no ip dhcp excluded-address`** command allows you to release previously excluded IP addresses for distribution to clients. No IP addresses are excluded by default. Up to 30 individual or ranges of IP addresses are supported. Example: **`ip dhcp excluded-address 132.53.4.2`** ***ip-addr*** – Specifies an IP address to exclude, or the first IP address in a range of excluded IP addresses. ***end-ip-addr*** – Specifies the last IP address in a range of excluded IP addresses.

Table C-9. DHCP Server Commands (2 of 3)

lease {*days*[*hours*] [*minutes*]| infinite} **no lease [*days*[*hours*] [*minutes*]|infinite]**
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to specify or clear the lease time for an IP address assigned to a DHCP client. After the lease time has expired, the address assignment is no longer valid. The default lease time is one day. Example: **lease 120 23 0** ***days*** – Number of days the lease is valid. The default is1. Valid range of days is 0–365. ***hours*** – Number of hours the lease is valid. The default is 0. Valid range for hours is 0–24. ***minutes*** – Number of minutes the lease is valid. The default is 0. Valid range for minutes is 0–59. **infinite** – Specifies an infinite lease time. The IP address assignment does not expire.
default-router *ip-address* **no default-router** [*ip-address*]
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to configure or remove the default router IP address provided to clients by the DHCP server. The default router address is provided to the clients in the DHCP reply message from the DHCP server and as the next hop router by the clients. The IP address for the default router should be on the same subnet as the client. Example: **default-router 132.53.4.2** ***ip-address*** – Specifies the IP address of the default router. The default is None.
domain-name *domain-name* **no domain-name** [*domain-name*]
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to specify or remove the domain name provided to clients by the DHCP server. This domain name is provided to the clients in the DHCP reply message from the DHCP server. ***domain-name*** – Specifies a string defining the domain name. The domain name string contains 255 ASCII printable characters. The default is None.
dns-server *ip-address* **no dns-server** [*ip-address*]
Minimum Access Level: **Administrator** Command Mode: **config-dhcp**
Allows you to specify or remove the Domain Name System (DNS) IP address provided to clients by the DHCP server. Example: **dns-server 132.53.4.2** ***ip-address*** – Specifies the IP address of the DNS server.

Table C-9. DHCP Server Commands (3 of 3)

network *network-num*
[[netmask] *netmask* **| {prefix-length |/}** *prefix-length***]**

no network [*network-num*
[[netmask] *netmask* **| {prefix-length |/}** *prefix-length***]]**

Minimum Access Level: **Administrator**
Command Mode: **config-dhcp**

Allows you to specify or remove a subnet and subnet mask to a DHCP server pool. The configured subnet and subnet mask will specify the range of IP addresses that will be allocated to clients by the DHCP server. Only one network or subnet may be specified for a server pool.

Example: **network 8**

network-num – The IP address of the DHCP address pool.

netmask – Specify a network mask that indicates which address bits belong to the network and subnet fields and which bits belong to the host field.

netmask – The network mask for the pool of IP addresses.

prefix-length or **/** – Specify the number of bits in a network mask address that are ones and define the network and subnet fields.

prefix-length – Number of ones bits in a network mask address. Valid range is 1–32.

NOTES:

– If the mask or prefix-length is not specified, the class A, B, or C natural mask is used.

– When the DHCP address range is changed, all binding entries and dynamic routes for the clients configured with the old address range are removed.

DHCP Relay Agent Commands

Dynamic Host Configuration Protocol (DHCP) relay agent commands

Table C-10. DHCP Relay Agent Commands

ip dhcp relay max-clients *max-dhcp-clients* **no ip dhcp relay max-clients [***max-dhcp-clients***]**
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to limit the number of DHCP clients supported. The **no dhcp relay max-agents** command resets the maximum number of DHCP clients supported to the default of 1. Example: **ip dhcp relay max-clients 1** ***max-dhcp-clients*** – Number of DHCP clients supported: 1–256.
[no] ip dhcp-server *ip-address*
Minimum Access Level: **Administrator** Command Mode: **config**
Allows you to specify or remove the address of the DHCP server where DHCP requests received on the Ethernet interface are forwarded. When no server address is assigned, the DHCP Relay agent is effectively disabled. NOTE: The DHCP Relay agent cannot be enabled if either the DHCP server or NAT are enabled. ***ip-address*** – IP address of the DHCP server.

Filter (access-list) Commands

Filter commands are used to create or delete Access Lists.

Table C-11. Filter Commands (1 of 4)

```
access-list access-list-num [{permit | deny}
     {{source-ip [source-wildcard] | any | host source-host-ip} |
     {protocol {source-ip source-wildcard | any | host source-host-ip}
          [src-operator src-port [src-end-port] ]
     {dest-ip dest-wildcard | any | host dest-host-ip}
          [ [icmp-msg-type [icmp-msg-code] ] |
          [dest-operator dest-port [dest-end-port] ] ] }|
     {type-code [range end-type-code] } }

no access-list access-list-num [{permit | deny}
     {{source-ip [source-wildcard] | any | host source-host-ip} |
     {protocol {source-ip source-wildcard | any | host source-host-ip}
          [src-operator src-port [src-end-port] ]
     {dest-ip dest-wildcard | any | host dest-host-ip}
          [ [icmp-msg-type [icmp-msg-code] ] |
          [dest-operator dest-port [dest-end-port] ] ] } |
     {type-code [ range end-type-code] } }
```

Minimum Access Level: **Administrator**
Command Mode: **config**

Allows a user to create or delete a rule for an access list. Access lists default to an implicit deny statement for everything. Access lists are terminated by an implicit deny.

access-list-num – The access list number. Valid ranges for access lists are:

- **1–99** – Standard IP access lists.
- **100–199** – Extended IP access lists.
- **200–299** – Protocol type-code access lists.

permit – Specifies to permit access and forward packets matching the criteria.

deny – Specifies to deny access and discard packets matching the criteria.

For Standard IP Access Lists:

Example: `access-list 1 permit 10.1.1.1`

source-ip – The source IP Address to match.

source-wildcard – Specifies a 32-bit wildcard mask indicating the bit positions in the source IP address to ignore during matches. This argument must be supplied when a source-ip address is specified.

any – Specifies to match any source host. A source-ip of 0.0.0.0 and a source-wildcard of 255.255.255.255 are specified.

host – Specify a single host source address to match.

source-host-ip – The source host IP address to match.

(Continued on next page)

Table C-11. Filter Commands (2 of 4)

(Continued from previous page)

For Extended IP Access Lists:

Example: `access-list 100 permit tcp 10.1.1.1 0.0.0.255 20.1.1.1 0.0.0.255`

protocol – The IP protocol to which the filter will be applied. The following protocols are supported:

ip – Filter applies to all IP packets (including but not limited to ICMP, TCP, and UDP).

icmp – Internet Control Message Protocol.

tcp – Transmission Control Protocol.

udp – User Datagram Protocol.

source-ip – The source IP Address to match.

source-wildcard – Specifies a 32-bit wildcard mask indicating the bit positions in the source IP Address to ignore during matches. This argument must be supplied when a *source-ip* address is specified.

any – Match any source host. A source-ip of 0.0.0.0 and a source-wildcard of 255.255.255.255 are specified.

host – Specify a single host source address to match.

source-host-ip – The source host IP address to match.

dest-ip – The destination IP Address to match.

dest-wildcard – Specifies a 32-bit wildcard mask indicating the bit positions in the destination IP Address to ignore during matches. This argument must be supplied when a dest-ip address is specified.

any – Specifies to match any destination host. A dest-ip of 0.0.0.0 and a dest-wildcard of 255.255.255.255 are specified.

host – Specify a single host address to match.

dest-host-ip – The destination host IP address to match.

icmp-msg-type – Specify a specific ICMP message type to be filtered. Valid if the protocol *s*pecified is icmp. For valid ICMP message types, refer to Table C-15, ICMP Designations. Valid ICMP message type range is 0–255.

icmp-msg-code – Specify a specific ICMP message code to be filtered. Valid if an icmp-msg-type has been specified and the protocol specified is icmp. For valid ICMP message codes, refer to Table C-15, ICMP Designations. Valid ICMP message type range is 0–255.

src-operator – Specifies how the source port is evaluated. This argument may only be specified if the protocol specified is tcp or udp. Valid values are:

eq – Match only packets with a port number equal to the source port number input.

gt – Match only packets with a port number greater than the source port number.

lt – Match only packets with a port number less than the source port number input.

neq – Match only packets with a port number not equal to the source port number.

range – Match only packets in the range of port numbers specified by src-port and src-end-port. If range is specified, enter both a src-port and a src-end-port.

(Continued on next page)

Table C-11. Filter Commands (3 of 4)

For Extended IP Access Lists: *(continued)*

src-port – Specify a TCP or UDP port number to be filtered. Valid if the protocol specified is tcp or udp. Refer to Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid port number range is 0–65535.

src-end-port – Specifies last TCP or UDP port number in a range of port numbers to be filtered. Valid if the protocol specified is tcp or udp and if src-operator value is range. Refer to Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid port number range is 0–65535.

dest-operator – Specifies how the destination port is evaluated. This argument may only be specified if the protocol specified is tcp or udp. Valid values are:

> **eq** – Match only packets with a port number equal to the destination port number.
>
> **gt** – Match only packets with a port number greater than the destination port number.
>
> **lt** – Match only packets with a port number less than the destination port number.
>
> **neq** – Match only packets with a port number not equal to the destination port number.
>
> **range** – Match only packets in the range of port numbers specified by dest-port and dest-end-port. If range is specified, enter both a dest-port and dest-end-port.

dest-port – Specifies a specific TCP or UDP port number to be filtered. This option only applies to a protocol of tcp or udp. Many of the valid TCP and UDP ports are described in Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid TCP or UDP port number range is 0–65535.

dest-end-port – Specifies last TCP or UDP port number in a range of port numbers to be filtered. This option only applies to a protocol of tcp or udp with dest-operator set to range. Many of the valid TCP and UDP ports are described in Table C-16, TCP Port Designations, and Table C-17, UDP Port Designations. Valid TCP or UDP port number range is 0–65535.

For Protocol Type Access Lists:

> Example: `access-list 200 permit 0x200 range 0x210`

type-code – Specifies the 16-bit hexadecimal number written with a leading “0x” that specifies either an Ethernet type code or the first Ethernet type code in a range of Ethernet type codes to filter. If a user attempts to a type code that is not a 16-bit hexadecimal number written with a leading “0x”, it will be treated as a syntax error. Many of the Ethernet Type codes distributed by the Xerox Corporation are listed in Table C-14, Ethernet Type Codes (Hex). This option only applies to protocol type-code access lists.

range – Specifies a range of ether-type codes. This option only applies to protocol type-code access lists.

> ***end-type-code*** – The last ethernet type code included in the filter range. A 16-bit hexadecimal number written with a leading “0x” used to specify one of the Ethernet type codes. This option only applies for protocol type-code access lists.

Table C-11. Filter Commands (4 of 4)

[no] `ip access-group` *access-list-1-199num* **`[in	out]`**
Minimum Access Level: Administrator Command Mode: config-if
Allows you to control access to an interface by allowing you to designate (or delete) a set of access rules to be applied to either incoming or outgoing packets. By default, no access lists are applied to interfaces. Example: ip access-group 17 in NOTE: A user may specify that an access list is applied to either inbound packets, outbound packets, or both inbound and outbound packets (two commands). If a specified access list does not exist, all packets are passed. access-list-1-199num – The access list number. The valid ranges for access lists are: **1–99** – Standard IP access lists. **100–199** – Extended IP access lists. **in** – Specifies that filters will be applied to inbound packets. **out** – Specifies that filters will be applied to outbound packets. If no direction (in or out) is specified, the filter is applies to outbound packets by default.

Diagnostic Commands

Diagnostic commands allow you to ping or trace the route to a specified destination.

Table C-12. Diagnostic Commands (1 of 2)

ping [*protocol***]** *dest-ip* **[source** *source-ip***] [length** *bytes***]**
[timeout *time***] [interface** *intf-type intf-num* **[.***sub-intf-num***]]**

Minimum Access Level: **Operator**
Command Mode: **Standard**

Pings the specified destination address.

For a successful ping, the results are shown as:

Ping reply [*x.x.x.x*]: bytes of data = *packet-length*

Where *packet-length* is the length of echo packets sent.

For a timeout, the results are shown as:

Ping reply [*x.x.x.x*]: REQUEST TIMED OUT

For an ICMP echo response of unreachable destination, the results are shown as:

Ping reply [*x.x.x.x*]: DESTINATION UNREACHABLE

protocol – The protocol of the IP echo message: ip.

dest-ip – Address of the device to ping.

source – Specify the source IP address.

source-ip – The source IP address used in the ping request. The default source IP address is the IP address for the interface on which packets are routed to the destination IP address. The source IP address specified must be an IP address assigned to an interface or sub-interface.

length – Specify the length of echo packets sent.

bytes – Number of data bytes. Range = 0–1500. Default = 64.

timeout – Specify the time in seconds before the ping test is abandoned.

time – Number in seconds before the ping test is abandoned. Maximum is 30 seconds. Default = 5 seconds.

interface – Specify the target interface. The default target interface is the interface on which packets are routed to the destination IP address.

intf-type – Two interface types are supported:

Ethernet – IEEE 802.3 interface

Serial – Frame relay serial interface

intf-num – The interface index number for the Ethernet and the Serial interfaces: 0.

sub-intf-num – The sub-interface number. Sub-interfaces are only supported on the Network interface (Serial 0). Sub-interface number range is 0–4,294,967,295.

Table C-12. Diagnostic Commands (2 of 2)

traceroute [protocol] *dest-ip* **[source** *source-ip***] [length** *bytes***]**
[timeout *time***] [hops** *hops***] [interface** *intf-type intf-num* **[.***sub-intf-num***]]**

Minimum Access Level: **Operator**
Command Mode: **Standard**

This command performs the TraceRoute test to the specified destination IP address. The general format of the TraceRoute results is seen as follows:

Tracing route to *x.x.x.x* over a max of *nn* hops, with *nnn* byte packet:

```
1   <100ms   <100ms   <100ms  x.x.x.x
2   <100ms   <100ms   <100ms  x.x.x.x
3   <200ms   <200ms   <200ms  x.x.x.x
4   <200ms   <200ms   <200ms  x.x.x.x
```

The first column is the hop number, which is the Time to Live (TTL) value set in the IP packet header. Each of the three next columns contains the round-trip time in 100ms intervals for each attempt to reach the destination with that TTL value. If no response is received, an * (asterisk) is displayed in place of the roundtrip time. The fifth column is the IP address of the responding system. If no response is received for a hop, the last column is blank.

protocol – The protocol of the echo message for TraceRoute: ip.

dest-ip – Address of the device to TraceRoute.

source – The source IP address. The default source IP address is the IP address for the interface on which packets are routed to the destination IP address.

> ***source-ip*** – The source IP address used in the TraceRoute test. The default source IP address will be the IP address for the interface on which packets are routed to the destination IP address. The source IP address specified must be an IP address assigned to an interface or sub-interface.

length – Specify the length of packets sent.

> ***bytes*** – Number of data bytes. Range = 0–1500. Default = 64.

timeout – Specify the time in seconds before the TraceRoute test is abandoned.

> ***time*** – Number of seconds before the TraceRoute test is abandoned. Range = 1–30. Default = 5 seconds.

hops – Specify the maximum number of hops to be tested.

> ***hops*** – The maximum number of hops to be tested. Range = 1–128. Default = 8.

interface – Specify the target interface. The default target interface is the interface on which packets are routed to the destination IP address.

> ***intf-type*** – Two interface types are supported:
>
> > **Ethernet** – IEEE 802.3 interface
> >
> > **Serial** – Frame relay serial interface
>
> ***intf-num*** – The interface index number for the Ethernet and the Serial interfaces: 0.
>
> ***sub-intf-num*** – The sub-interface number is only supported on the Network interface (Serial 0). The following sub-interface numbers are supported: 0–4,294,967,295.

Show Commands

Show commands allow you to display information.

Table C-13. Show Commands (1 of 4)

`show arp`

Minimum Access Level: **Operator**
Command Mode: **Standard**

Displays the devices in the ARP table.

The general format of the **`show arp`** command is:

IP Address	Timeout (min)	MAC address	Type	Interface
x.x.x.x	STATIC	*xx:xx:xx:xx:xx:xx*	ARPA	
x.x.x.x	*time*	*xx:xx:xx:xx:xx:xx*	ARPA	*Interface*

The first column displays the IP address. The second column displays the actual time left for the specific entry, or "STATIC" for configured static entries. The third column displays the MAC address for the ARP entry. The fourth column displays the ARP type (only ARPA is currently supported). The fifth column displays the Interface or sub-interface for the ARP table entry.

`show bridge`

Minimum Access Level: **Operator**
Command Mode: **Standard**

Displays entries in the bridge forwarding database.

`show configuration`

Minimum Access Level: **Operator**
Command Mode: **Standard**

Displays/outputs a sequence of commands in the form of ASCII strings that have the effect of setting all configurable parameters to the current values in memory.

Passwords are write-only and not output. The text file can be used with a terminal emulation program. Refer to *Configuring the Router Using Terminal Emulation* in Chapter 5, *Configuring the FrameSaver SLV Router.*

The general format of the **`show config`** command is:

```
global commands
  !
  interface n
   interface n commands....
  !
  interface n sub-interface n
   interface n sub-interface n commands...
  !
  interface n sub-interface n+1
   interface n sub-interface n+1 commands...
  interface n+1
```

Table C-13. Show Commands (2 of 4)

`show configuration {saved | unsaved}`
Minimum Access Level: **Administrator** Command Mode: **All config modes**
Displays/outputs a sequence of commands in the form of ASCII strings that have the effect of setting all configurable parameters to the current values, either saved in memory or entered during a current configuration session. Passwords are write-only and not output. The text file can be used with a terminal emulation program. Refer to *Configuring the Router Using Terminal Emulation* in Chapter 5, *Configuring the FrameSaver SLV Router*. The general format of the show config command is the same as the previous command, show configuration, in Standard mode. **saved** – Displays the command sequence for saving parameters currently saved in memory. **unsaved** – Displays the command sequence for saving parameters entered during the current configuration session.
`show frame-relay map`
Minimum Access Level: **Operator** Command Mode: **Standard**
Displays the status of all frame relay DLCIs seen on the router's frame relay interface. The general format of the **`show frame-relay map`** command is: *interface* **(***interface-status***):** dlci *dlci-number***,** *dlci-status* Where the *interface* (or sub-interface) shall be displayed in the standard format shown in the Interface Commands. The *interface-status* is up or down. The *dlci-number* is in the range 16–1007. Frame relay map statements are only displayed for DLCIs configured on both the router and on the devices user interface. The *dlci-status* is active or inactive.
`show interface` **[***intf-type intf-num* **[.***sub-intf-num***]]**
Minimum Access Level: **Operator** Command Mode: **Standard**
Shows the status of the named interface, sub-interface, or all interfaces and sub-interfaces on the device. ***intf-type*** – The interface type. The following two types are supported: **Ethernet** – IEEE 802.3 interface **Serial** – Serial interface ***intf-num*** – The interface index number for the Ethernet and the Serial interfaces: 0. ***sub-intf-num*** – The sub-interface numbers are only supported on the Network interface (Serial 0). Sub-interface numbers supported: 0–4,294,967,295.

Table C-13. Show Commands (3 of 4)

`show ip dhcp binding [`*ip-address*`]`

Minimum Access Level: **Operator**
Command Mode: **Standard**

Allows users to display address bindings associated with the DHCP server. If the IP address is not specified, all DHCP server bindings are displayed. If an IP address is specified, only the DHCP server binding for the specified client is displayed.

ip-address – Specifies the DHCP client's IP address for the binding to be displayed.

The general format of the **`show ip dhcp bindings`** command is as follows:

```
IP Address   MAC address       Lease Expires
x.x.x.x      xx:xx:xx:xx:xx:xx  ddd:hh:mm
```

The first column displays the IP addresses in use. The second column displays the MAC address bound to each IP address. The third column displays the remaining lease time in days, hours, and minutes or "Infinite".

`show ip nat translations`

Minimum Access Level: **Operator**
Command Mode: **Standard**

Shows the active Network Address Translation (NAT) translations. The general format of the **`show ip nat translations`** command is:

```
Pro   Inside global   Inside local   Outside local    Outside global
udp   x.x.x.x:port    x.x.x.x:port   x.x.x.x:port     x.x.x.x:port
```

The first column, Pro, displays the Protocol of the port identifying the address. The second column displays the Inside global IP address for one or more inside local IP addresses to the outside world. The third column displays the Inside local IP address assigned to a host on the inside network.

The fourth column displays the Outside local IP address of an outside host as it appears to the inside network. The fifth column displays the Outside global IP address assigned to a host on the outside network by its owner. Whenever one of the IP addresses or the Protocol designation does not apply to a NAT table entry, "---" is displayed. A protocol port is appended to IP addresses when NAPT is specified for that NAT entry.

`show ip route [`*ip-address*`]`

Minimum Access Level: **Operator**
Command Mode: **Standard**

This command shows the IP route table entry for the specified IP address. If no IP address is specified, the entire table is shown. When the Next Hop IP Address is 0.0.0.0, the host is directly reachable on the interface.

The general format of the **`show ip route`** command will be as follows:

```
Dest. IP Address   Dest. Subnet Mask   Next Hop IP Addr   Interface
x.x.x.x            x.x.x.x             x.x.x.x             interface
x.x.x.x             x.x.x.x            x.x.x.x            interface
```

ip-address – Specific IP address for route information display.

Table C-13. Show Commands (4 of 4)

`show ip traffic`
Minimum Access Level: **Operator** Command Mode: **Standard**
Displays the IP statistics for the device.
`show spanning-tree`
Minimum Access Level: **Operator** Command Mode: **Standard**
Displays the devices spanning-tree topology.

Ethernet Type Codes

Use Table C-14, Ethernet Type Codes (Hex), when specifying the filter applied to incoming Ethernet packets by Type Code. Many of the Type Codes listed below are distributed by Xerox Corporation.

Table C-14. Ethernet Type Codes (Hex) (1 of 2)

Type Code	Description	Type Code	Description
0000–05DC	IEEE802.3 Length Field	803E	DEC Unassigned
010101FF	Experimental	803F	DEC LAN Traffic Monitor
0200	Xerox PUP (see 0A00)	8040–8042	DEC Unassigned
0201	PUP Addr Trans (see 0A01)	8044	Planning Research Corp.
0600	Xerox NS IDP	8046–8047	AT&T
0800	DOD IP	8049	ExperData
0801	X.75 Internet	805B	Stanford V Kernel exp.
0802	NBS Internet	805C	Stanford V Kernel prod.
0803	ECMA Internet	805D	Evans & Sutherland
0804	Chaosnet	8060	Little Machines
0805	X.25 Level 3	8062	Counterpoint Computers
0806	ARP	8065–8066	University of Mass. at Amherst
0807	XNS Compatibility	8067	Veeco Integrated Auto.
081C	Symbolics Private	8068	General Dynamics
0888–088A	Xyplex	8069	AT&T
0900	Ungermann-Bass net debugger	806A	Autophon
0A00	Xerox IEEE802.3 PUP	806C	ComDesign
0A01	PUP Addr Trans	806D	Computgraphic Corp.
0BAD	Banyan Systems	80E–E8077	Landmark Graphics Corp.
1000	Berkeley Trailer nego	807A	Matra
1001–100F	Berkeley Trailer encap/IP	807B	Dansk Data Elektronik
1600	Valid Systems	807C	Merit Internodal
4242	PCS Basic Block Protocol	807D–807F	Vitalink Communications
5208	BBN Simnet	8080	Vitalink TransLAN III
6000	DEC Unassigned (Exp.)	8081–8083	Counterpoint Computers
6001	DEC MOP Dump/Load	809B	Appletalk
6002	DEC MOP Remote Console	809C–809E	Datability
6003	DEC DECNET Phase IV Route	809F	Spider Systems Ltd.

Table C-14. Ethernet Type Codes (Hex) (2 of 2)

Type Code	Description	Type Code	Description
6004	DEC LAT	80A3	Nixdorf Computers
6005	DEC Diagnostic Protocol	80A4–80B3	Siemens Gammasonics Inc. (Xerox)
6006	DEC Customer Protocol	80C0–80C3	DCA Data Exchange Cluster (Xerox)
6007	DEC LAVC, SCA	80C6	Pacer Software
6008–6009	DEC Unassigned	80C7	Applitek Corporation
6010–6014	3Com Corporation	80C8–80CC	Intergraph Corporation
7000	Ungermann-Bass download	80CD–80CE	Harris Corporation
7002	Ungermann-Bass dia/loop	80CF–80D2	Taylor Instrument
7020–7029	LRT	80D3–80D4	Rosemount Corporation
7030	Proteon	80D5	IBM SNA Service on Ether
7034	Cabletron	80DD	Varian Associates
8003	Cronus VLN	80DE–80DF	Integrated Solutions TRFS
8004	Cronus Direct	80E0–80E3	Allen-Bradley
8005	HP Probe	80E4–80F0	Datability
8006	Nestar	80F2	Retix
8008	AT&T	80F3	AppleTalk AARP (Kinetics)
8010	Excelan	80F4–80F5	Kinetics
8013	SGI diagnostics	80F7	Apollo Computer
8014	SGI network games	80FF–8103	Wellfleet Communications
8015	SGI reserved	8107–8109	Symbolics Private
8016	SGI bounce server	8130	Waterloo Microsystems
8019	Apollo Computers	8131	VG Laboratory Systems
802E	Tymshare	8137–8138	Novell, Inc.
802F	Tigan, Inc.	8139–813D	KTI
8035	Reverse ARP	814C	SNMP
8036	Aeonic Systems	9000	Loopback
8038	DEC LANBridge	9001	3Com(Bridge) XNS Sys Mgmt
8039–803C	DEC Unassigned	9002–9003	3Com(Bridge) TCP-IP Sys & loop detect
803D	DEC Ethernet Encryption	FF00	BBN VITAL-LanBridge cache

Protocol and Port Designations

The following tables are used for filtering.

ICMP Designations

Use the Internet Control Management Protocol (ICMP) designations in Table C-15, ICMP Designations, when specifying a specific ICMP message to be filtered.

Table C-15. ICMP Designations (1 of 2)

Type	Code	ICMP Message	Description
0	0	echo-reply	Echo (ping) reply
All 3*n* = Destination unreachable			
3	0	net-unreachable	Network unreachable
3	1	host-unreachable	Host unreachable
3	2	protocol-unreachable	Protocol unreachable
3	3	port-unreachable	Port unreachable
3	4	packet-too-big	Fragmentation needed and do not fragment (DF) bit set
3	5	source-route-failed	Source route failed
3	6	network-unknown	Destination network unknown
3	7	host-unknown	Destination host unknown
3	8	host-isolated	Source host isolated
3	9	dod-net-prohibited	Destination network admin prohibited
3	10	dod-host-prohibited	Destination host admin prohibited
3	11	net-tos-unreachable	Network unreachable for TOS (Type of Service)
3	12	host-tos-unreachable	Host unreachable for TOS
3	13	Administratively-prohibited	Communication admin. prohibited by filtering
3	14	host-precedence-unreachable	Host precedence violation
3	15	precedence-unreachable	Precedence cutoff in effect
4	0	source-quench	Source quench (flow control)

Table C-15. ICMP Designations (2 of 2)

Type	Code	ICMP Message	Description
All 5*n* = All redirects			
5	0	net-redirect	Redirect for network
5	1	host-redirect	Redirect for host
5	2	net-tos-redirect	Redirect for Type of Service (TOS) & network
5	3	host-tos-redirect	Redirect for Type of Service (TOS) & host
8	0	echo	Echo request (ping)
9	0	router-advertisement	Router discovery advertisements
10	0	router-solicitation	Router discovery solicitations
11	0	ttl-exceeded	TTL (Time to Live) = 0 & exceeded during transit (Traceroute)
11	1	reassembly-timeout	TTL (Time to Live) = 0 & exceeded during reassembly
12	0	general-parameter-problem	IP header bad
12	1	option-missing	Parameter required but not present
12	2	no-room-for-option	Parameter required but no room
13	0	timestamp-request	Timestamp request
14	0	timestamp-reply	Timestamp reply
15	0	information-request	Information request
16	0	information-reply	Information reply
17	0	mask-request	Address mask request
18	0	mask-reply	Address mask reply

TCP Port Designations

Use the Transmission Control Protocol (TCP) port designations in Table C-16, TCP Port Designations, when specifying a specific TCP port to be filtered.

Table C-16. TCP Port Designations

TCP Port #	TCP Port Table	Description
7	echo	Echo
9	discard	Discard
13	daytime	Daytime
19	chargen	Character generator
20	ftp-data	FTP data connections
21	ftp	File Transfer Protocol
23	telnet	Telnet
25	smtp	Simple Mail Transport Protocol
37	time	Time
43	whois	Nicname
49	tacacs	TAC Access Control System
53	domain	Domain Name Service
70	gopher	Gopher
79	finger	Finger
80	www	World Wide Web (HTTP)
101	hostname	NIC hostname server
109	pop2	Post Office Protocol v2
110	pop3	Post Office Protocol v3
111	sunrpc	Sun Remote Procedure Call
119	nntp	Network News Transport Protocol
179	bgp	Border Gateway Protocol
194	irc	Internet Relay Chat
512	exec	Exec (rsh)
513	login	Login (rlogin)
514	cmd	Remote commands (rcmd)
514	syslog	Syslog
515	lpd	Printer service
517	talk	Talk
540	uucp	UNIX-to-UNIX Copy Program
543	klogin	Kerberos login
544	kshell	Kerberos shell

UDP Port Designations

Use the User Datagram Protocol (UDP) port designations in Table C-17, UDP Port Designations, when specifying a specific UCP port to be filtered.

Table C-17. UDP Port Designations

UDP Port #	UDP Port Name	Description
7	echo	Echo
9	discard	Discard
37	time	Time
42	nameserver	IEN116 name service (obsolete)
49	tacacs	TAC Access Control System
53	domain	Domain Name Service (DNS)
67	bootpc	Bootstrap Protocol (BOOTP) client
68	bootps	Bootstrap Protocol (BOOTP) server
69	tftp	Trivial File Transfer Protocol
111	sunrpc	Sun Remote Procedure Call
123	ntp	Network Time Protocol
137	netbios-ns	NetBios name service
138	netbios-dgm	NetBios datagram service
161	snmp	Simple Network Management Protocol
162	snmptrap	SNMP Traps
177	xdmcp	X Display Manager Control Protocol
195	dnsix	DNSIX security protocol auditing
434	mobile-ip	Mobile IP registration
512	biff	Biff (mail notification, comsat)
513	who	Who service (rwho)
514	syslog	System Logger
517	talk	Talk
520	rip	Routing Information Protocol

Router Command Line Summaries and Shortcuts

D

CLI Summaries

For summaries of Command Line Interface commands, see:

- Table D-1, Show Commands
- Table D-2, Access Control and System Level Commands
- Table D-3, CLI Commands

  For default settings, see *CLI Command Default Settings* on page D-6.

The minimal characters that must be typed when entering commands are shown in **`courier bold`** for these tables.

For details on each command and the conventions used for command line syntax, see Appendix C, *Router CLI Commands, Codes, and Designations.*

Show Command Summary

Table D-1, Show Commands, lists all of the show, or display, commands for the CLI.

Table D-1. Show Commands

Command	Function
show **a**rp	Displays all the devices in the router's ARP table.
show **b**ridge	Displays the router's bridge forwarding database entries.
show **c**onfiguration	Displays the router's current configuration.
show **c**onfiguration {**s**aved|**u**nsaved}	Shows the current configuration, either saved in memory or entered during the current session.
show **f**rame-relay **m**ap	Shows the status of all frame relay DLCIs on the router's frame relay interface.
show **in**terface [*intf-type intf-num* [.*sub-intf-num*]]	Shows the status of the specified interface, sub-interface, or all interfaces and sub-interfaces for the router.
show **ip d**hcp **b**inding [*ip-address*]	Shows the address bindings associated with the DHCP server. ■ If an IP address is specified, only bindings for that client will be displayed. ■ If no IP address is specified, all DHCP server bindings are displayed.
show **ip n**at **t**ranslations	Displays all the address bindings associated with the DHCP server.
show **ip r**oute [*ip-address*]	Shows the Routing Table entry for the device with the specified IP address, or all Routing Table entries if no IP address is specified.
show **ip t**raffic	Shows IP statistics for the router.
show **s**panning-tree	Displays the router's spanning-tree topology.

Access Control and System Level Command Summary

Table D-2, Access Control and System Level Commands, lists of all of the access control and system level commands for the CLI.

Table D-2. Access Control and System Level Commands

Command	Function
?	Displays all valid commands for the current access level.
!	Used to enter comments. Comments following the ! are ignored by the CLI.
configure {**t**erminal|**f**actory)	Enters configuration mode so configuration options can be edited.
disable	Exits Administrator access level.
enable	Enters/enables the Administrator access level.
enable **p**assword *password* **no** **en**able **p**assword [*password*]	Sets or disables the password level. Default is None.
end	Leaves configuration mode to return to standard operating mode.
exit	Leaves the current configuration level or terminates the session. It may be necessary to enter the exit command several times when leaving configuration mode.
help	Displays a summary of help options.
[**n**o] **pa**ger	Enables/Outputs up to 23 lines.
reload	Resets the router and reloads its configuration.
save	Saves changes to the router's configuration.

CLI Command Summary

Table D-3, CLI Commands lists of all of the system-level commands for the CLI. For the default settings, see *CLI Command Default Settings* on page D-6.

Table D-3. CLI Commands (1 of 2)

Command
access-list *access-list-num* [{permit | deny} { {*source-ip* [*src-wildcard*] | any | host *source-host-ip*} | {*protocol* {*source-ip source-wildcard* | any | host *source-host-ip*} [*src-operator src-port* [*src-end-port*]] {*dest-ip dest-wildcard* | any | host *dest-host-ip*} [[*icmp-msg-type* [*icmp-msg-code*]] | [*dest-operator dest-port* [*dest-end-port*]]] } | {*type-code* [**r**ange *end-type-code*] } } **no ac**cess-list *access-list-num* [{permit | deny} { {*src-ip* [*src-wildcard*] | any | host *src-host-ip*} | {*protocol* {*src-ip src-wildcard* | any | host *src-host-ip*} [*src-operator src-port* [*src-end-port*]] {*dest-ip dest-wildcard* | any | host *dest-host-ip*} [[*icmp-msg-type* [*icmp-msg-code*]] | [*dest-operator dest-port* [*dest-end-port*]]] } | {*type-code* [**r**ange *end-type-code*] }]
arp *ip-address mac-address arp-type* **n**o **ar**p *ip-address* [*mac-address arp-type*]
arp **t**imeout *time* **n**o **ar**p **t**imeout [*time*]

bridge {**c**rb | *bridge-group* {**ac**quire | **ag**ing-time *aging-time* |
protocol *span-tree-protocol* | **pri**ority *span-tree-priority* | **r**oute *route-protocol*} }
no bridge {**c**rb | *bridge-group* {**ac**quire | **ag**ing-time [*aging-time*] |
priority [*span-tree-priority*] | **r**oute [*route-protocol*] } }

[**no**] **b**ridge-group *bridge-group*
[**n**o] **b**ridge-group *bridge-group* {**i**nput-type-list *in-access-list-200num* | **o**utput-type-list *out-access-list-200num*}
clear **a**rp-cache
clear **c**ounters [*intf-type intf-num* [.*sub-intf-num*]]
clear **ip n**at **t**ranslations *
default-router *ip-address* **n**o **d**efault-router [*ip-address*]
dns-server *ip-address* **n**o **dn**s-server [*ip-address*]
domain-name *domain-name* **n**o **do**main-name [*domain-name*]

Table D-3. CLI Commands (2 of 2)

Command
encapsulation *encapsulation-type encapsulation-protocol*
[**n**o] **f**rame-relay **i**nterface-dlci *dlci-num*
interface *intf-type intf-num* [.*sub-intf-num* [**p**oint-to-point]] **n**o **in**terface *intf-type intf-num.sub-intf-num* [**p**oint-to-point]
ip address *ip-addr subnet-mask* **n**o **ip ad**dress [*ip-addr subnet-mask*]
[**n**o] **ip ac**cess-group *access-list-1-199num* [**i**n | **o**ut]
[**n**o] **ip dhcp p**ool *pool-name*
ip dhcp relay **m**ax-clients *max-dhcp-clients* **n**o **ip dhcp r**elay **m**ax-clients [*max-dhcp-clients*]
[**n**o] **ip dhcp-s**erver *ip-address*
[**n**o] **ip m**ulticast-routing
[**n**o] **ip n**at {**i**nside | **o**utside}
[**n**o] **ip n**at **i**nside **s**ource {**l**ist *access-list-1–99num* **p**ool *pool-nam*e [**o**verload] | **l**ist *access-list-1–99num* **i**nterface *intf-type intf-num* [.*sub-intf-num*] **o**verload | **s**tatic {*static-ip-addr1 static-ip-addr2* | *protocol static-ip-addr1 static-port-num static-ip-addr2*} }
[**n**o] **ip n**at **p**ool *pool-name start-ip-addr end-ip-addr* {**n**etmask *netmask* | {**p**refix-length | / } *prefix-length*}
ip nat **t**ranslation **t**imeout *time* **n**o **ip n**at **t**ranslation **t**imeout [*time*]
ip route *dest-ip dest-mask* {*next-hop-ip* | *intf-type intf-num* [.*sub-intf-num*] } **n**o **ip route** *dest-ip dest-mask* [*next-hop-ip* | *intf-type intf-num* [.*sub-intf-num*]]
[**n**o] **ip routi**ng
[**n**o] **ip un**numbered [**n**ull **0**]
lease {*days* [*hours*] [*minutes*] | **i**nfinite} **n**o lease [*days* [*hours*] [*minutes*] | **i**nfinite]
network *network-num* [[**n**etmask] *netmask* | {**p**refix-length | / } *prefix-length*] **n**o **ne**twork [*network-num* [[**n**etmask] *netmask* | {**p**refix-length | / } *prefix-length*]]
ping [*protocol*] *dest-ip* [**s**ource *source-ip*] [**l**ength *bytes*] [**t**imeout *time*] [**i**nterface *intf-type intf-num* [.*sub-intf-num*]]
[**n**o] **se**rvice dhcp
traceroute [*protocol*] *dest-ip* [**s**ource *source-ip*] [**l**ength *bytes*] [**t**imeout *time*] [**h**ops *hops*] [**i**nterface *intf-type intf-num* [.*sub-intf-num*]]

CLI Command Default Settings

The following list shows the default settings:

```
!software version d1.06.04
!
no enable password
ip routing
no ip multicast-routing
service dhcp
ip nat translation timeout 86400
ip dhcp relay max-clients 256
bridge 1 acquire
bridge 1 aging-time 300
bridge 1 protocol ieee
bridge 1 priority 32768

interface Ethernet 0
 bridge-group 1
 arp timeout 14400
!
interface Serial 0
 Encapsulation frame-relay ietf
 bridge-group 1
!
end
```

Connectors, Cables, and Pin Assignments

E

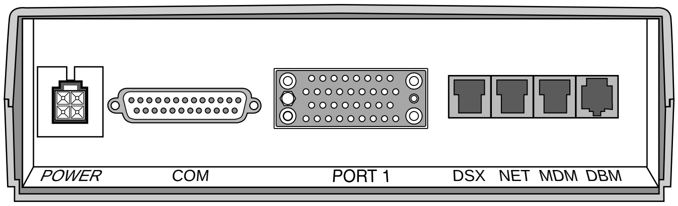
This appendix shows the FrameSaver unit rear panels, and pin assignments for the connectors/interfaces and cables. Standard interfaces are used on the unit, so most cables do not have to be specially ordered; they can be purchased anywhere.

NOTE:

In the pin assignment tables of this appendix, if the pin number is not shown, it is not being used.

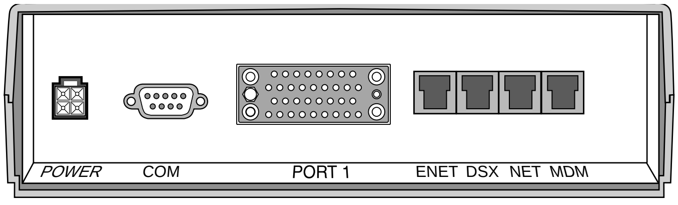
Rear Panels

The following illustration shows the rear panel of the FrameSaver SLV 9126 (without Ethernet).



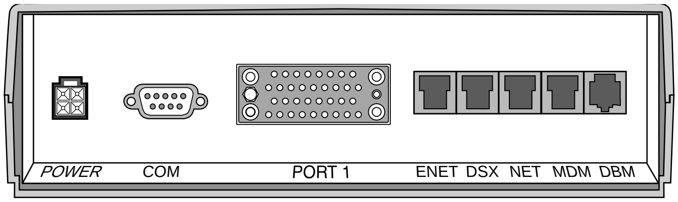
98-16154

The following illustration shows the rear panel of the FrameSaver SLV 9126-II (with Ethernet) and the 9126-II Router.



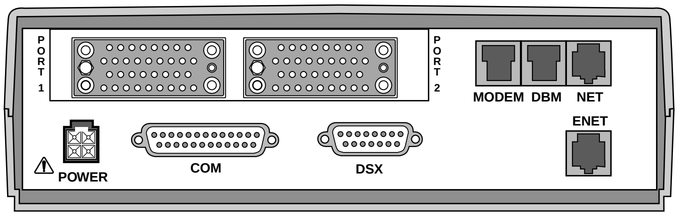
02-17141a

The following illustration shows the rear panel of the FrameSaver SLV 9126-II (with Ethernet and DBM).



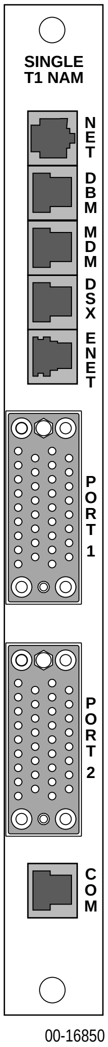
02-17141

The following illustration shows the rear panel of a 1-slot FrameSaver SLV 9128-II.



00-16840

The following illustration shows the rear panel of the carrier-mounted, single T1, dual port FrameSaver SLV 9128-II.



Model 9128-II

The sections that follow provide pin assignments for each interface.

COM Port Connector

The type of COM port connector depends on the model.

COM Port for 9126 and 9128-II (25-Position)

The following table provides the pin assignments for the FrameSaver SLV 9126 and 9128-II units' 25-position EIA-232C communication port connector.

Signal	Direction	Pin #
Shield (GND)	—	1
DCE Transmit Data (TXD)	From DTE (In)	2
DCE Receive Data (RXD)	To DTE (Out)	3
DCE Request to Send (RTS)	From DTE (In)	4
DCE Clear to Send (CTS)	To DTE (Out)	5*
DCE Data Set Ready (DSR)	From DTE (In)	6*
Signal Ground (SG)	—	7
DCE Carrier Detect (CD)	To DTE (Out)	8*
DCE Data Terminal Ready (DTR)	From DTE (In)	20

* Pins 5, 6, and 8 are tied together.

COM Port for 9126-II (9-Position)

The following table provides the pin assignments for the 1-slot FrameSaver SLV 9126-II's 9-position EIA-232C communication port connector.

Pin #	Signal	Direction
1*	Data Carrier Detect (DCD)	To DTE (Out)
2	Receive Data (RD)	To DTE (Out)
3	Transmit Data (TD)	From DTE (In)
4	Data Terminal Ready (DTR)	From DTE (In)
5	Signal Ground (GND)	—
6*	Data Set Ready (DSR)	To DTE (Out)
7	Not used	—
8*	Clear To Send (CTS)	To DTE (Out)
9	Not used	—

*Pins 1, 6, and 8 are tied together.

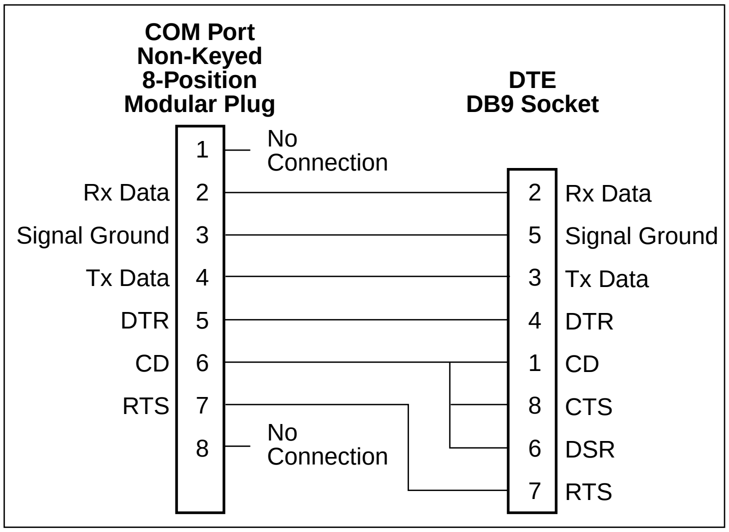
COM Port for 9128-II Carrier Mount

The following table shows the signals and pin assignments for the carrier-mounted FrameSaver SLV 9128-II NAM's 8-position communication port interface/connector.

Signal	Direction	Pin #
DCE Received Data (RXD)	From DCE (Out)	2
Signal Ground (SG)	To/From DCE	3
DCE Transmit Data (TXD)	To DCE (In)	4
DCE Data Terminal Ready (DTR)	To DCE (In)	5
DCE Carrier Detect (CD)	From DCE (Out)	6
DCE Request to Send (RTS)	To DCE (In)	7

COM Port-to-PC Cable (Feature No. 3100-F2-550)

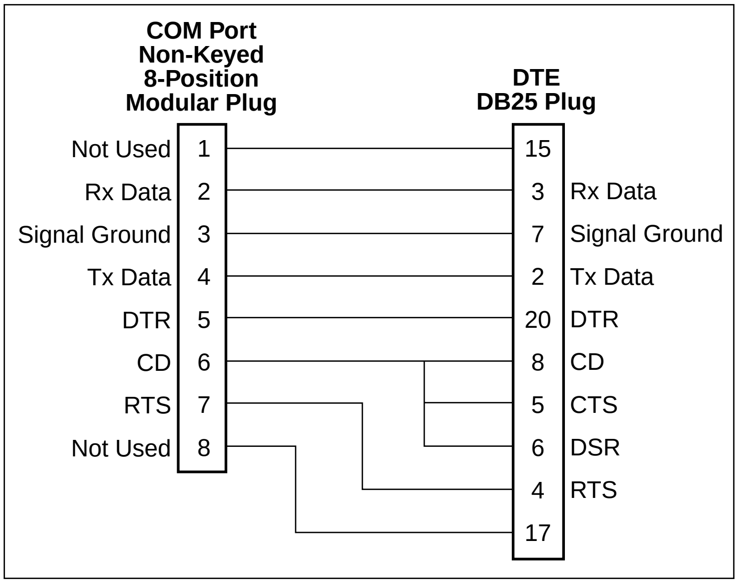
Order this cable when connecting the 8-position COM port to a PC. The following shows the pin assignments from the COM port to the DTE interface.



98-16166

COM Port-to-Terminal/Printer Cable (Feature No. 3100-F2-540)

Order this cable when connecting the 8-position COM port to a terminal or printer, rather than to a PC. The following shows the pin assignments from the COM port to the DTE interface.



98-16167

COM Port-to-Router Cables

The following tables provide the pin assignments for connecting the 1-slot FrameSaver unit's 25-position communication port to various router auxiliary (AUX) or console ports using standard cables.

Cisco 2500 Series Router – RJ45 Jack

COM Port			AUX Port	
Signal	**DB25 Pin #**	**Direction**	**RJ45 Pin #**	**Signal**
DCE Transmit Data (TXD)	2	To DTE	3	DTE Transmit Data (TXD)
DCE Receive Data (RXD)	3	From DTE	6	DTE Receive Data (RXD)
DCE Request to Send (RTS)	4	To DTE	1	DTE Request to Send (RTS)
DCE Clear to Send (CTS)	5	From DTE	8	DCE Clear to Send (CTS)
DCE Data Set Ready (DSR)	6	From DTE	7	DCE Data Set Ready (DSR)
DCE Signal Ground (SG)	7	—	4, 5	DTE Signal Ground (SG)
DCE Data Terminal Ready (DTR)	20	To DTE	2	DTE Data Terminal Ready (DTR)

Cisco 7000 Series Router – DB25 Plug

COM Port			AUX Port	
Signal	**DB25 Pin #**	**Direction**	**DB25 Pin #**	**Signal**
DCE Transmit Data (TXD)	2	To DTE	2	DTE Transmit Data (TXD)
DCE Receive Data (RXD)	3	From DTE	3	DTE Receive Data (RXD)
DCE Request to Send (RTS)	4	To DTE	4	DTE Request to Send (RTS)
DCE Signal Ground (SG)	7	—	7	DTE Signal Ground (SG)
DCE Carrier Detect (CD)	8	To DTE	8	DTE Carrier Detect (CD)
DCE Data Terminal Ready (DTR)	20	To DTE	20	DTE Data Terminal Ready (DTR)

3COM Router – DB9 Socket

COM Port			Console Port	
Signal	**DB25 Pin #**	**Direction**	**DB9 Pin #**	**Signal**
DCE Transmit Data (TXD)	2	To DTE	3	DTE Transmit Data (TXD)
DCE Receive Data (RXD)	3	From DTE	2	DTE Receive Data (RXD)
DCE Request to Send (RTS)	4	To DTE	7	DTE Request to Send (RTS)
DCE Signal Ground (SG)	7	—	5	DTE Signal Ground (SG)
DCE Carrier Detect (CD)	8	To DTE	1	DTE Carrier Detect (CD)
DCE Data Terminal Ready (DTR)	20	To DTE	4	DTE Data Terminal Ready (DTR)

The following tables provide the pin assignments for connecting the FrameSaver SLV 9128-II NAM's 8-position communication port to various router auxiliary (AUX) or console ports using standard cables.

Cisco 2500 Series Router – RJ45 Jack

COM Port			AUX Port	
Signal	**RJ45 Pin #**	**Direction**	**RJ45 Pin #**	**Signal**
DCE Receive Data (RXD)	2	From DTE	6	DTE Receive Data (RXD)
DCE Signal Ground (SG)	3	—	4, 5	DTE Signal Ground (SG)
DCE Transmit Data (TXD)	4	To DTE	3	DTE Transmit Data (TXD)
DCE Data Terminal Ready (DTR)	5	To DTE	2	DTE Data Terminal Ready (DTR)
DCE Request to Send (RTS)	7	To DTE	1	DTE Request to Send (RTS)

Cisco 7000 Series Router – DB25 Plug

COM Port			AUX Port	
Signal	**RJ45 Pin #**	**Direction**	**DB25 Pin #**	**Signal**
DCE Receive Data (RXD)	2	From DTE	3	DTE Receive Data (RXD)
DCE Signal Ground (SG)	3	—	7	DTE Signal Ground (SG)
DCE Transmit Data (TXD)	4	To DTE	2	DTE Transmit Data (TXD)
DCE Data Terminal Ready (DTR)	5	To DTE	20	DTE Data Terminal Ready (DTR)
DCE Carrier Detect (CD)	6	To DTE	8	DTE Carrier Detect (CD)
DCE Request to Send (RTS)	7	To DTE	4	DTE Request to Send (RTS)

3COM Router – DB9 Socket

COM Port			AUX Port	
Signal	**RJ45 Pin #**	**Direction**	**DB25 Pin #**	**Signal**
DCE Receive Data (RXD)	2	From DTE	2	DTE Receive Data (RXD)
DCE Signal Ground (SG)	3	—	5	DTE Signal Ground (SG)
DCE Transmit Data (TXD)	4	To DTE	3	DTE Transmit Data (TXD)
DCE Data Terminal Ready (DTR)	5	To DTE	4	DTE Data Terminal Ready (DTR)
DCE Carrier Detect (CD)	6	To DTE	1	DTE Carrier Detect (CD)
DCE Request to Send (RTS)	7	To DTE	7	DTE Request to Send (RTS)

Gender Adapter/Changer

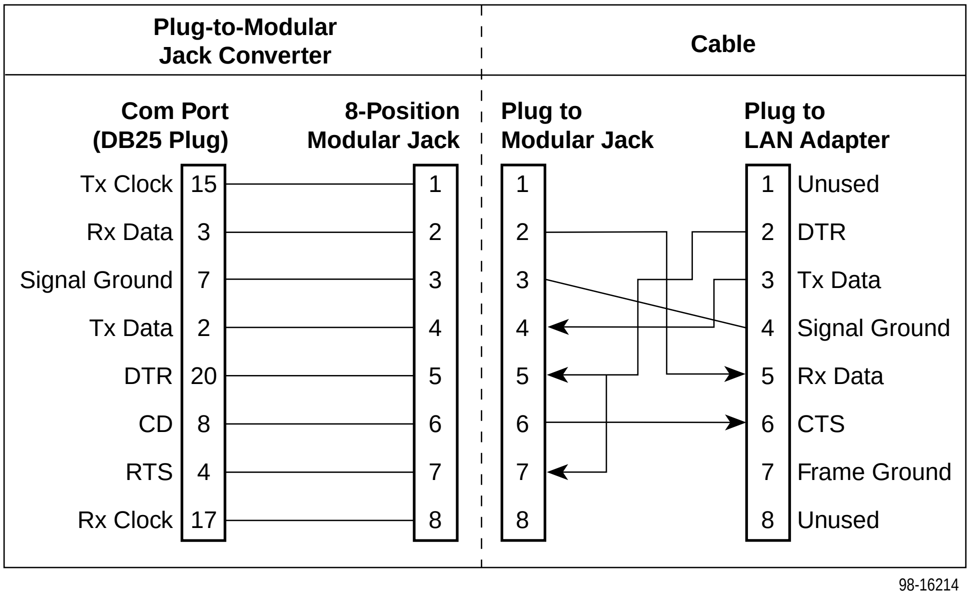
When connecting the COM port to a router or Frame Relay Assembler/ Disassembler (FRAD), a gender adapter is required to convert the COM Port-to-Terminal/Printer cable's plug-type interface to a socket-type interface for the router's or FRAD's AUX port.

LAN Adapter Converter and Cable

A LAN adapter converter and cable is not needed for the FrameSaver SLV 9128-II carrier-mounted unit, and cannot be used with the FrameSaver SLV 9126-II.

The following shows the pin assignments for the:

- DB25 plug-to-modular jack converter between the COM port and the 8-conductor LAN Adapter cable (Feature No. 3100-F2-920)
- Custom 8-conductor cable (with modular plugs on both ends) between the converter and the LAN Adapter (Feature No. 3100-F2-910)



DTE Port Connector

The following table provides the pin assignments for the 34-position V.35 connector to the DTE.

Signal	ITU CT#	Direction	34-Pin Socket
Shield	101	—	A
Signal Ground/Common (SG)	102	—	B
Request to Send (RTS)	105	To DSU (In)	C
Clear to Send (CTS)	106	From DSU (Out)	D
Data Set Ready (DSR)	107	From DSU (Out)	E
Receive Line Signal Detector (RLSD or LSD)	109	From DSU (Out)	F
Data Terminal Ready (DTR)	108/1, /2	To DSU (In)	H
Local Loopback (LL)	141	To DSU (In)	L
Transmit Data (TXD)	103	To DSU (In)	P (A) S (B)
Receive Data (RXD)	104	From DSU (Out)	R (A) T (B)
Transmit Signal Element Timing – DTE Source (XTXC or TT)	113	To DSU (In)	U (A) W (B)
Receive Signal Element Timing – DCE Source (RXC)	115	From DSU (Out)	V (A) X (B)
Transmit Signal Element Timing – DCE Source (TXC)	114	From DSU (Out)	Y (A) AA (B)
Test Mode Indicator (TM)	142	From DSU (Out)	NN

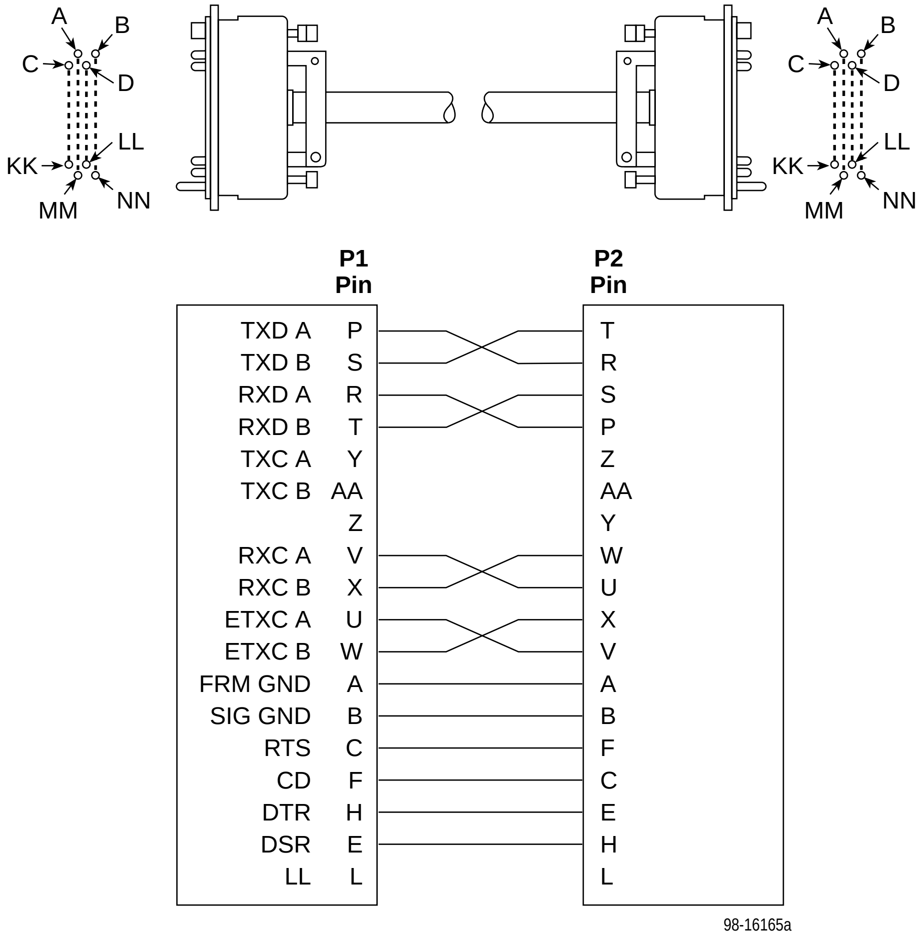
Standard V.35 Straight-through Cable

A standard V.35 straight-through cable can be used to connect a DTE port to a DTE, where a 34-pin plug-type connector is needed for the data port and a 34-position socket-type connector is needed for the DTE. No special-order cables are required.

Standard V.35 Crossover Cable

A standard V.35 crossover cable with a 34-pin plug-type connector on each end of the cable can be used to connect the FrameSaver unit's DTE port to another DCE.

The following illustration provides the pin assignments for the V.35 crossover cable.



	P1 Pin	P2 Pin
TXD A	P	T
TXD B	S	R
RXD A	R	S
RXD B	T	P
TXC A	Y	Z
TXC B	AA	AA
	Z	Y
RXC A	V	W
RXC B	X	U
ETXC A	U	X
ETXC B	W	V
FRM GND	A	A
SIG GND	B	B
RTS	C	F
CD	F	C
DTR	H	E
DSR	E	H
LL	L	L

DSX-1 Connector

The type of DSX-1 port connector depends on the model.

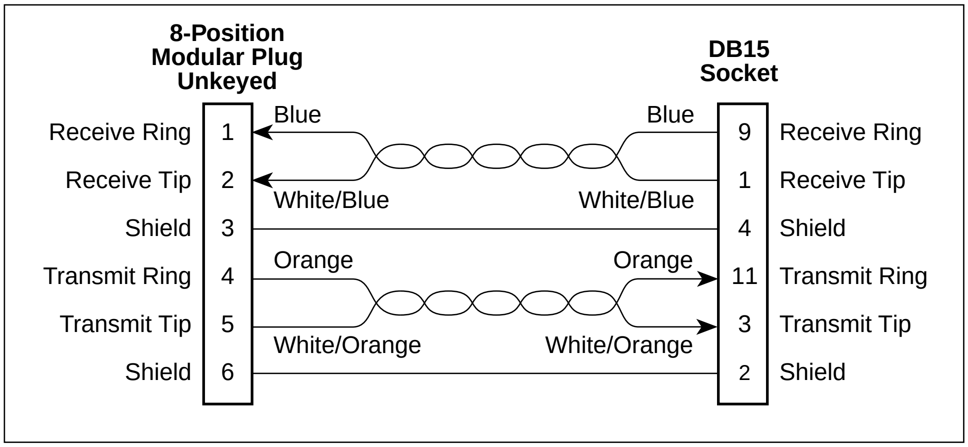
DSX-1 Port for 9126, 9126-II, and Carrier Mounted 9128-II (8-Position)

The following table shows the signals and pin assignments for the 8-position modular DSX-1 interface on the FrameSaver SLV 9126, 9126-II, and 9128-II carrier-mounted units. The DSX-1 Adapter is required for this interface.

Function	Circuit	Direction	Pin Number
Receive Ring	R1	From DTE	1
Receive Tip	T1	From DTE	2
Shield	—	—	3
Transmit Ring	R	To DTE	4
Transmit Tip	T	To DTE	5
Shield	—	—	6

DSX-1 Adapter (Feature No. 9008-F1-560)

The DSX-1 adapter cable is used as an interface between the FrameSaver unit's DSX-1 connector and the DTE's DB15 interface. The following shows pin assignments and the purpose of each.



99-16216a

DSX-1 Port for 1-Slot 9128-II (15-Position)

The following table shows the signals and pin assignments for the 15-position DSX-1 interface on the FrameSaver SLV 9128-II standalone units. A DSX-1 adapter is not required for this interface.

Function	Circuit	Direction	Pin Number
Receive Tip	T1	From DTE	1
Transmit Tip	T	To DTE	3
Shield	—	—	2, 4
Receive Ring	R1	From DTE	9
Transmit Ring	R	To DTE	11

T1 Network Cable (Feature No. 3100-F1-500)

Network access is via a 20-foot cable with an RJ48C unkeyed plug-type connector on each end. The following table shows pin assignments and the purpose of each.

Function	Circuit	Direction	Pin Number
Receive Ring	R1	From Network	1
Receive Tip	T1	From Network	2
Transmit Ring	R	To Network	4
Transmit Tip	T	To Network	5

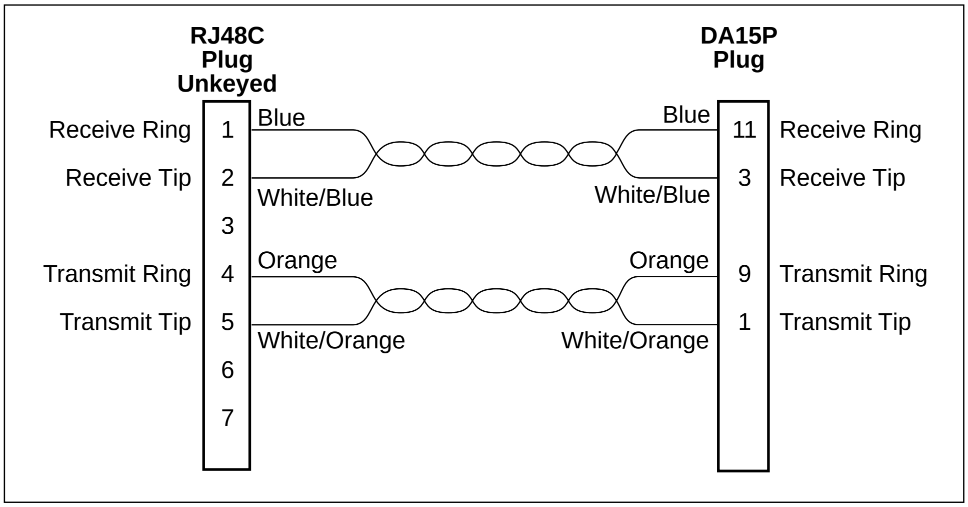
T1 Mass Termination Cable (Feature No. 9007-F1-500)

The following pin assignments are for the T1 Mass Termination cable that connects multiple carrier-mounted FrameSaver units to an M66 block. It has a 50-pin RJ48H plug at one end and seven RJ48C plugs at the other end.

Function	Circuit	Line #	Pin #	Function	Circuit	Line #	Pin #
Receive ring from the network	R1	1	1	Transmit ring to the network	R	1	14
		2	2			2	15
		3	3			3	16
		4	4			4	17
		5	5			5	18
		6	6			6	19
		7	7			7	20
Receive tip from the network	T1	1	26	Transmit tip to the network	T	1	39
		2	27			2	40
		3	28			3	41
		4	29			4	42
		5	30			5	43
		6	31			6	44
		7	32			7	45

Canadian T1 Line Interface Cable (Feature No. 3100-F1-510)

The T1 line interface cable is used in Canada as an interface between the FrameSaver unit's network connector and the T1 network interface. The following shows pin assignments and the purpose of each.



98-16215

Ethernet Port Connector

The following table provides the pin assignments for the FrameSaver unit's Ethernet port 8-position unkeyed modular jack.

Signal	Direction	Pin #
10/100 BaseT Transmit Data (TD +)	To LAN Interface (Out)	1
10/100 BaseT Transmit Data (TD –)	To LAN Interface (Out)	2
10/100 BaseT Receive Data (RD +)	From LAN Interface (In)	3
10/100 BaseT Receive Data (RD –)	From LAN Interface (In)	6

Modem Connector

The dial modem interface/connector that is integrated into the FrameSaver unit is an RJ11 6-position, 4-contact unkeyed modular jack. The following table shows pin assignments and the purpose of each.

Function	Circuit	Direction	Pin Number
Ring	R	To Local Loop	2
Tip	T	To Local Loop	3

ISDN DBM Connector

The backup connection is through the DBM interface/connector, which is an 8-position keyed modular jack. The following tables show pin assignments for the ISDN PRI and BRI DBMs and the purpose of each.

FrameSaver SLV 9128-II ISDN PRI pin assignments:

Function	Circuit	Direction	Pin Number
PRI Receive Ring	DBM1	From Local Loop	1
PRI Receive Tip	DBM2	From Local Loop	2
PRI Transmit Ring	DBM4	To Local Loop	4
PRI Transmit Tip	DBM5	To Local Loop	5

FrameSaver SLV 9126 ISDN BRI/U pin assignments:

Function	Circuit	Direction	Pin Number
BRI Transmit/Receive Ring	DBM4	To/From Local Loop	4
BRI Transmit/Receive Tip	DBM5	To/From Local Loop	5

ISDN Modular Cable

The ISDN cable comes with the FrameSaver unit ordered with the DBM feature.

Technical Specifications

F

The following technical specifications are included:

- NAM Technical Specifications (Table F-1)
- 1-Slot CSU/DSUs and Router Technical Specifications (Table F-2)
- 14-Slot 9000 Series Access Carrier Technical Specifications (Table F-3)
- ISDN BRI DBM (Optional Feature) Technical Specifications (Table F-4)
- ISDN PRI DBM (Optional Feature) Technical Specifications (Table F-5)

Table F-1. NAM Technical Specifications (1 of 3)

Specification	Criteria
Approvals	
FCC Part 15	Class A digital device
FCC Part 68	Refer to the equipment's label for the Registration Number.
Industry Canada	Refer to the equipment's label for the Certification Number.
Safety	Refer to the equipment's label for safety information.
Physical Environment	
Operating temperature	32°F to 122°F (0°C to 50°C)
Storage temperature	–4°F to 158°F (–20°C to 70°C)
Relative humidity	5% to 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Physical Dimensions	
NAM	
Height	8 inches (20.32 cm)
Depth	11.58 inches (29.41 cm)
I/O Card	
Height	10.15 inches (25.78 cm)
Depth	2.9 inches (7.37 cm)

Table F-1. NAM Technical Specifications (2 of 3)

Specification	Criteria
Weight	
NAM	1 lb. 2 oz. (.51 kg)
I/O Card	6 oz. (.17 kg)
Power Consumption and Dissipation	9.5 watts, 0.080 A at 120 VAC Result: 32 Btu per hour
COM Port/Interface – Communications/Management	8-position unkeyed modular jack
Standard	EIA-232/ITU, V.24 (ISO 2110)
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 Kbps
T1 Network Interface	8-position unkeyed modular USOC RJ48C jack
Data rates	Up to 1.536 Mbps
Services supported	Fractional T1 service, frame relay service
Physical interface (USA)	RJ48C
Physical interface (Canada)	CA81A using adapter cable
Framing format	D4, ESF
Coding format	AMI, B8ZS
Line Build-Out (LBO)	0.0 dB, –7.5 dB, –15 dB, –22.5 dB
ANSI PRM	Selectable
Bit stuffing	AT&T TR 62411
DSX-1 Interface	8-position modular connector with 8-position modular-to-DB15 adapter: D-Sub 15 socket
Framing format	D4, ESF
Coding format	AMI, B8ZS
DTE line equalization	5 selectable ranges from 0 to 655 feet (0 – 196.5 meters)
Send AIS	Selectable
Data Port	34-position V.35 connector
Standard	V.35/ITU (ISO 2593)
Data rates	Variations for T1 rates; automatically set to the network rate.
Modem (MDM) Interface	6-position unkeyed modular USOC RJ11C jack
Data rates	Up to 14.4 Kbps
Link Protocol	PPP, SLIP

Table F-1. NAM Technical Specifications (3 of 3)

Specification	Criteria
ISDN PRI DBM Interface	8-position unkeyed modular USOC RJ48C jack
Service supported	PRI, NI-1 or NI-2
Data rates	1.536 Kbps
Framing format	D4, ESF
Coding format	B8ZS
Line Build-Out (LBO)	0.0 dB, -7.5 dB, -15 dB, -22.5 dB
ANSI PRM	Selectable
Ethernet Port	8-position modular unkeyed jack
Standard	ANSI/IEEE Standard 802.3, Ethernet Version 2
Data rates	10/100 BaseT (auto-sensing 10 and 100 Mbps Ethernet rates

Table F-2. 1-Slot CSU/DSUs and Router Technical Specifications (1 of 3)

Specification	Criteria
Approvals	
FCC Part 15	Class A digital device
FCC Part 68	Refer to the equipment's label for the Registration Number.
Industry Canada	Refer to the equipment's label for the Certification Number.
Safety	Refer to the equipment's label for safety information.
Physical Environment	
Operating temperature	32°F to 122°F (0°C to 50°C)
Storage temperature	–4°F to 158°F (–20°C to 70°C)
Relative humidity	5% to 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Physical Dimensions	
Height	2.9 inches (7.4 cm)
Width	8.5 inches (21.6 cm)
Depth	12.5 inches (31.8 cm)
Weight	
FrameSaver SLV 9126	2.10 lbs. (0.95 kg)
FrameSaver SLV 9126-II and 9126-II Router	2.65 lbs. (1.2 kg)
FrameSaver SLV 9128-II	2.59 lbs. (1.18 kg)

Table F-2. 1-Slot CSU/DSUs and Router Technical Specifications (2 of 3)

Specification	Criteria
Power Consumption and Dissipation	
Built-in power cord	NEMA 5-15P plug
100–240 VAC power supply:	
FrameSaver SLV 9126	9.1 watts, 60 Hz ±3, 0.151 A at 120 VAC ±12 Result: 31.05 BTU per hour
120 VAC power supply:	
FrameSaver SLV 9126-II and 9126-II Router	7.3 watts, 60 Hz ±3, 0.131 A at 120 VAC ±12 Result: 24.9 BTU per hour
FrameSaver SLV 9128-II	10.3 watts, 60 Hz ±3, 0.125 A at 120 VAC ±12 Result: 35.14 BTU per hour
COM Port/Interface – Communications/Management	25-position (DB25) connector (9126, 9128-II) 9-position (DB9) connector (9126-II and 9126-II Router)
Standard	EIA-232/ITU, V.24 (ISO 2110)
Data rates	9.6, 14.4, 19.2, 28.8, 38.4, 57.6, and 115.2 Kbps
T1 Network Interface	8-position unkeyed modular USOC RJ48C jack
Data rates	Up to 1.536 Mbps
Services supported	Fractional T1 service, frame relay service
Physical interface (USA)	RJ48C
Physical interface (Canada)	CA81A using adapter cable
Framing format	D4, ESF
Coding format	AMI, B8ZS
Line Build-Out (LBO)	0.0 dB, –7.5 dB, –15 dB, –22.5 dB
ANSI PRM	Selectable
Bit stuffing	AT&T TR 62411
DSX-1 Interface	
Physical interface	
FrameSaver SLV 9126, 9126-II, and 9126-II Router	8-position modular connector with 8-position modular-to-DB15 adapter: D-Sub 15 socket
FrameSaver SLV 9128-II	15-position D-Subminiature connector D-Sub 15 socket
Framing format	D4, ESF
Coding format	AMI, B8ZS
DTE line equalization	5 selectable ranges from 0 to 655 feet (0 – 196.5 meters)
Send AIS	Selectable

Table F-2. 1-Slot CSU/DSUs and Router Technical Specifications (3 of 3)

Specification	Criteria
Data Port	34-position V.35 connector
Standard	V.35/ITU (ISO 2593)
Data rates	Variations for T1 rates; automatically set to the network rate.
Modem (MDM) Interface	6-position unkeyed modular USOC RJ11C jack
Data rates	Up to 14.4 Kbps
Link Protocol	PPP, SLIP
ISDN BRI DBM Interface	8-position keyed modular USOC RJ49C jack
Service supported	BRI, NI-1
Data rates	56 Kbps and 64 Kbps
ISDN PRI DBM Interface (FrameSaver SLV 9128-II only)	8-position unkeyed modular USOC RJ48C jack
Service supported	PRI, NI-1 or NI-2
Data rates	1.536 Kbps
Framing format	D4, ESF
Coding format	B8ZS
Line Build-Out (LBO)	0.0 dB, –7.5 dB, –15 dB, –22.5 dB
ANSI PRM	Selectable
Ethernet Port (FrameSaver SLV 9126-II, 9126-II Router, and 9128-II)	8-position modular unkeyed jack
Standard	ANSI/IEEE Standard 802.3, Ethernet Version 2
Data rates	10/100 BaseT (auto-sensing 10 and 100 Mbps Ethernet rates

Table F-3. 14-Slot 9000 Series Access Carrier Technical Specifications (1 of 2)

Specification	Criteria
Approvals	
FCC Part 15	Class A digital device
FCC Part 68	Refer to the equipment's label for the registration number.
Industry Canada	Refer to the equipment label for the certification number.
NRTL/C and CSA	Refer to the equipment label.

Table F-3. 14-Slot 9000 Series Access Carrier Technical Specifications (2 of 2)

Specification	Criteria
Physical Environment	
Operating temperature	35°F to 122°F (1.7°C to 50°C)
Storage temperature	–4°F to 158°F (–20°C to 70°C)
Relative humidity	5% to 85% (noncondensing)
Shock and vibration	Withstands normal shipping and handling
Physical Dimensions	
Height	10.5 inches (26.7 cm) or 6U
Width	17.2 inches (43.7 cm)
Depth	14.3 inches (36.3 cm)
Weight	Empty access carrier (without power supply)
	11 lbs. 6 oz. (5.16 kg)
AC Power Requirements	
AC Power Supply	90 to 265 VAC, 50/60 Hz ±3A maximum
DC Power Supply	–48 VDC, 6.6 amps, 316 watts
Heat Dissipation (Max.)	Fully loaded access carrier
227 VAC	585 Btu per hour maximum
–48 VDC	465 Btu per hour maximum
Typical Power Consumption	
AC Power Supply	
1 power supply installed	100 VAC 60 Hz 1.7 amps 171 watts 120 VAC 60 Hz 1.03 amps 60 watts 100 VAC 50 Hz 1.15 amps 60 watts Result: 207 Btu per hour
2 power supplies installed	100 VAC 60 Hz 1.25 amps 64.5 watts 120 VAC 60 Hz 1.5 amps 177 watts 230 VAC 50 Hz 0.9 amps 172 watts Result: 221 Btu per hour
DC Power Supply	
1 power supply installed	104 watts at –48 VDC Result: 355 Btu per hour
2 power supplies installed	124 watts at –48 VDC Result: 423 Btu per hour

Table F-4. ISDN BRI DBM (Optional Feature) Technical Specifications

Specification	Criteria
Standards Compliance	ANSI T1.601 – 1992 (physical layer) Bellcore SR-NWT-001937, Issue 1 – February 1991 ITU Q.921 – 1992 (link layer) ITU Q.931 – 1993 (network layer) TR-TSY-00860, ISDN Calling Number Identification Services – February 1989, and Supplement – June 1990
Power Consumption	60 mA at 15 VDC Average power .9 watt (3.07 Btu per hour)
Weight	0.27 lbs. 4.3 oz. (0.12 kg 122 grams)
Switch Compatibility	National ISDN-1 (NI-1)
Service Supported	Capability Package IOC B for 1B-service, which supports up to two circuit-switched B-channels, BRI-B1 and BRI-B2, with one Service Profile Identification (SPID) number and one local phone number. Capability Package IOC R for 2B-service, which supports up to two circuit-switched B-channels, BRI-B1 and BRI-B2, with two SPID numbers and two local phone numbers.
Switched Network Interface	One USOC RJ49C 8-pin keyed modular plug and jack, specified in ISO/IEC 8877
Transmit Interface	
Signal Level	13.5 dBm nominal over frequency band, 0 Hz – 80 kHz
Impedance	135 Ω
Receive Interface	
Dynamic Range	Operates on 2-wire loops, defined in ANSI T1.601-1992
Impedance	135 Ω
Modulation and Frequency	2B1Q line coding with 4-level amplitude modulation (PAM) at 80 Kbps baud
Channel Equalization	
Receiver	Automatic adaptive equalizer with echo cancellation

Table F-5. ISDN PRI DBM (Optional Feature) Technical Specifications

Specification	Criteria
Standards Compliance	ANSI T1.403 – 1989 (physical layer) and AT&T 62411 Bellcore SR-NWT-002120, Issue 1 – May 1992 ITU Q.921 – 1992 (link layer) ITU Q.931 – 1993 (network layer) TR-TSY-00860, ISDN Calling Number Identification Services – February 1989, and Supplement – June 1990
Power Consumption	8 mA at 120 VAC Average power 1 watt (3.4 Btu per hour)
Weight	0.15 lbs. 2.4 oz. (0.07 kg 68 grams)
Switch Compatibility	National ISDN-2 (NI-2), ATT 4ESS, or ATT 5ESS
Service Supported	PRI, NI-2, ATT 4ESS custom, or ATT 5ESS custom (supporting up to 23 B-channels), with Circuit-Switched Data capability.
Framing Format	D4, ESF
Coding Format	B8ZS
Line Build-Out (LBO)	0.0 dB, –7.5 dB, –15 dB, –22.5 dB
ANSI PRM	Selectable

Equipment List

G

Equipment

See *Cables* on page G-6 for cables you can order.

Description	Model/Feature Number
FrameSaver SLV Units	
FrameSaver SLV 9126 T1 remote site unit with: ■ SLM Feature Set ■ Integral modem ■ Support for up to 16 PVCs Includes 1-Slot Housing, Universal 100–240 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.	9126-A1-201
FrameSaver SLV 9126 T1 remote site unit with ■ SLM Feature Set ■ Integral modem ■ ISDN BRI DBM ■ Support for up to 16 PVCs Includes 1-Slot Housing, Universal 100–240 VAC Power Supply, Network Cable, RJ49C BRI ISDN/U Cable, Installation Instructions, and Quick Reference.	9126-A1-202
FrameSaver SLV 9126-II T1 remote site unit with: ■ SLM Feature Set ■ Integral modem ■ Support for up to 64 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.	9126-A2-201

Description	Model/Feature Number
FrameSaver SLV Units *(continued)*	
FrameSaver SLV 9126-II T1 remote site unit with: ■ SLM Feature Set ■ Integral modem ■ ISDN BRI DBM ■ Support for up to 64 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, RJ49C BRI ISDN-V Cable, Installation Instructions, and Quick Reference.	9126-A2-202
FrameSaver SLV 9126-II T1 remote site unit with: ■ Diagnostic Feature Set ■ Integral modem ■ Support for up to 64 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.	9126-A2-211
FrameSaver SLV 9126-II T1 Router with: ■ Diagnostic Feature Set ■ Integral modem ■ Support for up to 8 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.	9126-A2-214
FrameSaver SLV 9126-II T1 Router with: ■ SLM Feature Set ■ Integral modem ■ Support for up to 8 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.	9126-A2-224

Description	Model/Feature Number
FrameSaver SLV Units *(continued)*	
FrameSaver SLV 9128-II T1 central site 1-slot unit with: ■ SLM Feature Set ■ Integral modem ■ ISDN PRI DBM ■ Support for up to 120 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, RJ48C PRI ISDN Cable, Installation Instructions, and Quick Reference.	9128-A2-202
FrameSaver SLV 9128-II T1 central site 1-slot unit with: ■ SLM Feature Set ■ Integral modem ■ Support for up to 120 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.	9128-A2-204
FrameSaver SLV 9128-II T1 central site 1-slot unit with: ■ SLM Feature Set ■ Integral modem ■ Support for up to 120 PVCs ■ ISDN BRI DBM ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, ISDN BRI DBM, RJ49C BRI ISDN Cable, Installation Instructions, and Quick Reference.	9128-A2-204 with 9098-F1-870
FrameSaver SLV 9128-II T1 central site 1-slot unit with: ■ Diagnostic Feature Set ■ Integral modem ■ Support for up to 120 PVCs ■ Ethernet port for management Includes 1-Slot Housing, 120 VAC Power Supply, Network Cable, Installation Instructions, and Quick Reference.	9128-A2-211

Description	Model/Feature Number
FrameSaver SLV Units *(continued)*	
FrameSaver SLV 9128-II T1 central site carrier NAM with: ■ Diagnostic Feature Set ■ Integral modem ■ Support for up to 120 PVCs ■ Ethernet port for management Includes Network Cable, Installation Instructions, and Quick Reference.	9128-B2-211
FrameSaver SLV 9128-II T1 central site carrier NAM with: ■ SLM Feature Set ■ Integral modem ■ Support for up to 120 PVCs ■ Ethernet port for management Includes Network Cable, Installation Instructions, and Quick Reference.	9128-B2-212
FrameSaver SLM Feature Set Upgrade	
FrameSaver SLM Feature Set Activation Certificate for 9126	9126-C1-220
FrameSaver SLM Feature Set Activation Certificate for 9128	9128-C1-220
User Manual	
FrameSaver SLV, Models 9126, 9126-II, and 9128-II CSU/DSU and 9126-II Router, User’s Guide (Paper Manual)	9128-A2-GB20
NMS Products	
OpenLane Enterprise	7805-D1-001
OpenLane Workgroup	7805-D1-003
Optional Features	
Wall Mounting Kit for 1-Slot Housing	9001-F1-891
Shelf Mounting Kit for Up to Two 1-Slot Housings	9001-F1-894
ISDN BRI DBM	9098-F1-870
ISDN PRI DBM	9098-F1-875
Power Supplies	
100 – 240 VAC for 1-Slot Housing	9001-F1-040
120 VAC for 1-Slot Housing	9001-F1-020
AC Power Supply for Access Carrier	9007-F1-040
DC Power Supply for Access Carrier	9005-F1-050

Description	Model/Feature Number
9000 Series Access Carrier (9128-II NAM only)	
Access Carrier *Includes 14-Slot Housing, Universal 90 – 250 VAC Power Supply, Power Supply Tray, Baffle, Fan Tray, Mounting Brackets, and Installation Instructions.*	9007-B1-409
Access Carrier *Includes 14-Slot Housing, Universal –48 VDC Power Supply, Power Supply Tray, Baffle, Fan Tray, Mounting Brackets, and Installation Instructions.*	9007-B1-509
Baffle for Access Carrier	9007-S1-897
Fan Tray for Power Supply in Access Carrier	9007-S1-898
Fan Tray for Access Carrier	9007-S1-899

Cables

This table lists cables you can order.

Description	Part Number	Feature Number
RJ48C DSX-1 Network Cable, 8-pin modular-to-8-pin modular – 20 feet/6.1 meters	035-0209-2031	3100-F1-500
RJ48C T1 Network Cable, RJ48C-to-RJ48C – 20 feet/6.1 meters	035-0209-2031	3100-F1-500
T1 Line Interface Cable, RJ48C-to-CA81A – 20 feet/6.1 meters *For use in Canada.*	035-0221-2031	3100-F1-510
COM Port-to-LAN Adapter Cable, custom unkeyed 8-pin plug-to-8-pin plug modular cable – 14 feet/4.3 meters *Used for a LAN Adapter (LANA).*	035-0315-1431	3100-F1-910
Adapter, DB25 plug-to-8-pin modular receptacle *Used with the COM Port-to-LAN Adapter Cable.*	002-0069-0031	3100-F1-920
COM Port-to-Terminal Cable, 8-pin modular-to-DB25P – 14 feet/4.3 meters	035-0314-1431	3100-F2-540
COM Port-to-PC Cable, D-Sub9-to-DB25 for PC serial port – 14 feet/4.3 meters	035-0313-1431	3100-F2-550
T1 Mass Termination Cable, 50-pin plug-to-seven RJ48S plugs – 5 feet/1.5 meters *Connects carrier-mounted units to a M66 block.*	035-0363-0531	9007-F1-500
Adapter, 8-pin modular plug to DB15 jack *Used for DSX-1 interface.*	035-0386-0031	9008-F1-560
DSX-1 Adapter Cable, RJ48C-to-DB15 – 1 foot/0.3048 meters *For use by FrameSaver 9126, 9126-II, and carrier-mounted 9128.*	035-0386-0031	9008-F1-560

Index